WFH & Mobility Infrastructure Policy Bundle

2023 Edition

Janco Associates, Inc.

License Conditions

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the rights to use it for a SINGLE enterprise in a single county unless they have a multi-use license. Anyone who makes copies of or uses the template or any derivative of it is in violation of the United States and International copyright laws and subject to fines that are treble damages as determined by the courts. A REWARD of up to 1/3 of those fines will be anyone reporting such a violation upon the successful prosecution of such violators.

The purchaser agrees that derivative of this template will contain the following words within the first five pages of that document. The words are:

Published by: **Janco Associates Inc.**
Park City, UT 84098

435 940-9300 -- Email – support@e-janco.com

The publisher cannot in any way guarantee the procedures and approaches presented in this book are being used for the purposes intended and therefore assumes no responsibility for their proper and correct use. In addition, we are not attorneys and are not providing a legal opinion as to the data that should be retained nor the time periods that the data should be retained. The user should check with their own legal counsel to determine the specific requirements for record retention and destruction.

Printed in the United States of America

Contents

Work From Home & Mobiliy Infrastrcture Policy Bundle

Overview

Business mobile usage is exploding and becoming an increasingly powerful tool for marketers to connect with consumers around the world. Statistics show that professional text message use is expected to continue growing through the end of this decade. Although few in-depth studies focused on text messaging statistics have been done in the past, recent reports are beginning to shed light on the opportunities and help us grasp the size and potential impact on businesses.

- 5 billion people globally send and receive SMS messages.
- Over 300 million people in North America use text messages
- The mobile industry had a revenue of $3 trillion last year
- 3.3 billion people access the internet via mobile. It's predicted that by 2025, 72.6% of internet users will access the web via mobile-only, using their smartphones.
- 4 billion people are expected to own a smartphone by the end of the decade

Policies

This document contains the following policies:

- BYOD Access and Use Policy
- Mobile Device Access and Use Policy
- Privacy Compliance Policy
- Record Management, Retention, and Disposition Policy
- Social Networking Policy
- Travel, Laptop, PDA and Off-Site Meeting Policy
- Wearable Device Policy
- WFH and Telecommuting Policy

In addition, along with the 8 policies, included are electronic forms and full job descriptions to assist in the administration and management of the mobile workforce.

Job Descriptions

- Chief Mobility Officer
- Chief Security Officer
- Data Protection Officer
- Manager BYOD Support
- Manager Compliance
- Manager Record Administrator
- Manager Security and Workstations
- Manager Social Networking
- Manager Telecommuting
- Manager WFH Support
- BYOD Support Supervisor
- BYOD Support Specialist
- Record Management Coordinator
- Security Architect
- Social Media Specialist

Electronic forms

- Disaster Recovery foms
  - Remote Location Contact information
- Records Management
  - Administrative Records
  - Computer and Information Secuity Records
  - Computer Operations and Technical Support Records
  - Data Administratio Records
  - Facility Records
  - Financial Records
  - General Systems and Application Development Records
  - Mobile Device Access and Use Agrement
  - Network and Communication Services Records
  - Personell Records
  - Safety Records
  - Sales Reccords
  - User and Office Automation Records
- Safety Program
  - Inspection Checklist Work from Home Location
- Security
  -
  - Mobile Device Access and Use Agreement
  - Mobile Device Security and Compliance Checklist
  - Privacy Policy Compliance Agreement
  - Security Access Application
  - Sensitve Information Policy Compliance Agreement
  - Telecommution Work Agreement
  - Text Messaging Sensitve Information Agreement
  - Work From Home Work Agreement
- General forms
  - BYOD Access and Use Agreement
  - Company Asset Employee Control Log
  - Internet and Electronic Communication
  - Social Networking Policy Compliance Agreement
  - Telecommuting IT Checklist
  - Telecommuting Work Agreement
  - Wearable Device Access and Use Agreement
  - Work From Home IT Checklist

BYOD Policy Template

Janod Associates, Inc.

2023 Edition

License Conditions

Published by: **Janco Associates Inc.**
Park City, UT 84060

Email – support@e-janco.com

Table of Contents

Bring Your Own Device (BYOD) Access and Use Policy

Overview

The purpose of this policy is to define standards, procedures, and restrictions for end-users who have specific and authorized business requirements to access enterprise data from a personal device - BYOD (Bring Your Own DEVICE) - connected via a wired, wireless, or unmanaged network outside of ENTERPRISE's direct control. This policy applies to, but is not limited to, all devices and media that fit the following device classifications:

- Smartphones
- PDAs
- USB devices and data
- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Wearable devices
- Home or personal computers used to access enterprise resources
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

The policy applies to any hardware and related software that could be used to access enterprise resources, even when the equipment is not approved, owned, or supplied by ENTERPRISE.

Once you implement a BYOD policy, it's important to have a written agreement in place with every mobile device user. An agreement raises consciousness about the critical nature of mobile IT operations, and it protects organizations in the event of a BYOD policy violation. Like your BYOD policy itself, this agreement should be as clear as possible, to prevent misunderstandings that could generate a wide range of problems and IT headaches.

Components of the BYOD Strategy and Basics for BYOD Policy

The BYOD strategy and resultant policy are driven by 8 factors: device choice options; user experience and privacy; internal marketing and training; liability; economics; application design and infrastructure; maintainability; and trust security compliance. Each of these factors has been considered in the creation of this policy. A detailed description of each of these factors is provided later in this policy. Everyone in the company must be on the same page about what you can and can't access on personal devices. Policy guidelines need to be clear and compliance mandatory.

Device Choices

- Analyze employee preferences and understand which devices they already have
- Definite an acceptance baseline of what security and supportability features a bring-your-own-device program should support
- Understand the operating system, hardware, and regional variances around that baseline
- Develop an “easy” certification process for the evaluation of future devices
- Establish clear communication to users about which devices are allowed or not, and why
- Policies need to be established for device features from Global Positioning System (GPS) receivers to cameras and audio recorders. Policies should cover the use of these features as they relate to work.

User Experience and Privacy

- Identify activities and data IT will monitor
- Clarify the actions IT will take and under which circumstances
- Define the BYOD privacy policy
- Access security policies and restrictions for sustainability
- Deploy core services (email, critical apps, WLAN access) to the BYOD
- Preserving the native experience – do not force legacy application structure on BYOD

Trust Security Compliance

- Identify and assess the risk associated with security issues on BYOD
- Identify and define remediation options (notification, access control, quarantine, selective wipe)
- Set policy based on organizational hierarchy
- Establish a process to identify both the user and device
- Communicating compliance issues clearly to the employee
- Focus on the sustainability of the security policy being instituted
- Create policies regarding the usage of insecure Wi-Fi networks that make provisions for the limitations of their security measures. Some networks could be labeled off-limits, based on security alerts.

Application Design and Infrastructure

- Design BYOD applications to match the trust level of individual BYOD
- Modify the applications catalog availability based on device ownership
- Commit to the resource investment of building applications with BYOD in mind
- Update the application's acceptable-use policies
- Define enforcement levels for application violations (notification, access control, quarantine, or selective wipe or disable)
- Coordinate data created and modified with the ENTERPRISE records management procedures and processes
- Coordinate with HR and legal departments on termination issues with individuals who have used BYOD - including processes for lost devices.

Economics

- Shift the cost of device hardware to the user and move to a fixed fee per month paid to the user
- Control excess service charges through managed usage
- Establish service plans with outside entities, realizing some negotiating leverage might be lost
- Assess the productivity impact of users being able to use their desired platforms
- Change the help desk model (with BYOD, employees use the help desk as the last resort instead of a first resort)
- Access compliance and audit costs
- Assess tax implications both to the company and the individual

Liability

- Define the elements of the minimum protection for enterprise data on BYOD devices
- Assess liability for personal web and application usage
- Assess liability for usage onsite vs. offsite, and inside work hours vs. outside work hours
- Evaluate whether the nature of BYOD reimbursement affects liability (partial payment vs. full payment of service costs)
- Plan and budget for monitoring, enforcement, and audit of the BYOD compliance policy
- Assess the risk and resulting liability for accessing and damaging personal data (for example, doing a full wipe instead of a selective wipe by mistake)

Maintainability

- Define patch and version control for both software and firmware
- Securing corporate data and meeting ongoing mandated compliance requirements
- Minimize the cost of implementation and enforcement
- Preserve the native user experience
- Stay up-to-date with user preferences and technology innovations

Internal marketing and training

- Communicate why the company is moving to BYOD
- Understand BYOD is an HR initiative as much as an IT initiative
- Define IT's "brand" and level of service to be provided
- Supporting the brand message with the appropriate action
- Develop training materials for both the user and the helpdesk
- Provide 7x24 access to support via the help desk or recommended service providers

Device Ownership Issues

Although the era of the company-owned and company-provisioned mobile device seems to be ending, there's still an ownership issue -- or at least a permissions issue -- to be addressed. These issues apply to more than just mobile devices, though it's a rare company that seems to think them through for employees' home PCs and the like, which face the same fundamental issues.

Organizations in government, health care, and defense especially face the legal question of who needs to own the device, though the concern isn't exclusive to them. There's no clear answer to that question as yet, but the underlying issue concerns when ownership is necessary to gain management control. But more conservative organizations often decide they need legal ownership of the device.

- **Shared management.** The organization's contractor and employment policies boil down to "if you access business resources from a personal device, you give us the right to manage, lock, and even wipe that device, even if you end up losing personal data and apps as a result." This is often modified with a written agreement that spells out management expectations for both parties.
- **Corporate ownership and provisioning.** The organization buys and owns the device, even if it allows nonbusiness use on it. Employees who don't like the phone service on such devices (they may not get free minutes when calling family members and friends) are free to carry a personal device as well that has no corporate access.
- **Legal transfer.** The organization buys the device from the user. In some cases, that ownership is permanent -- a surefire way to dissuade employees from participating. In other cases, the organization buys the device for a token amount (say, a dollar) and gives the user the right to use it for personal purposes, then commits to selling it back for the same price when the employee leaves the organization. That's more likely to gain user acceptance than a one-way purchase.

A US Supreme Court 9-0 ruling declared that employees are not entitled to privacy if they use an employer’s issued device, so what level of privacy is there for BYODs? Will employees using BYODs be entitled to privacy if they are conducting business for their employers? Or will the employees using BYODs be entitled to privacy if the employer reimburses the employee for the cost(s) of the BYOD?

Policy

Access to the enterprise's fixed and wireless network, including the Internet, with BYOD (Bring Your Own Devices) shall be made available to employees, associates, and business partners primarily for operational and administrative purposes and per ENTERPRISE's policies, procedures, and mandated requirements. All data, applications, and network access information (i.e. VPN) associated with ENTERPRISE shall remain the property of ENTERPRISE and will be treated in such a way that it complies with all published and/or communicated policies and procedures of ENTERPRISE. Limited personal access to the network shall be permitted if the use:

- Imposes no tangible cost to ENTERPRISE;
- Does not unduly burden ENTERPRISE's computer or network resources;
- Have no adverse effect on an employee's job performance

Access to ENTERPRISE's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all regulations governing the use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with ENTERPRISE policies.

Upon an employee's termination (voluntary or involuntary) the employee-owned device is to be provided to their supervisor to ensure that all company-owned data (i.e. contacts, emails, files, etc), applications, and network access information and tools are removed.

Violations of law may result in criminal prosecution as well as disciplinary action by ENTERPRISE.

Device Requirements

The policy of ENTERPRISE is that these users must follow ENTERPRISE policies and procedures to support the management, tracking, securing, and supporting of these devices, just like they do for any other corporate computing platform.

Specifically, the policies that apply to these types of devices are:

- Security best practices for tablets include the use of multilevel passwords and device certificates, and the ability to remotely wipe the device if it is lost or stolen.
- Utilize tiered access to network resources to secure critical data and applications.
- Comply with application delivery mechanisms.
- Synchronize the BYOD to the corporate network at least weekly or whenever connected to ENTERPRISE's network
- Create an enciphered backup of the BYOD on a schedule that is approved by the CIO (Chief Information Officer)

Policy Definitions

The following are definitions that apply to this policy:

- **Wireless Network** - A connection point that allows two or more computers, to communicate, (enabling file sharing, printer sharing, internet connection, etc.), using standard protocol but without the use of network cabling and typically outside of ENTERPRISE's control
- **Employee** - An employee, contractor, associate, and others who work away from his/her central workplace either at home or at another ENTERPRISE-designated or approved remote work location utilizing a BYOD.
- **BYOD** – A device that employee uses to connect or use ENTERPRISE applications or data that is their personal device.

Access Control

- The CIO and Information Technology group reserve the right to refuse, by physical and non-physical means, the ability to connect BYODs to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the enterprise's systems, data, users, and clients at risk.
- ENTERPRISE reserves the right to install a "self-destruct" code on the device which can be activated remotely or when a breach or other event occurs. ENTERPRISE is NOT responsible or liable for any damage or inconvenience that this can cause to BYOD or its owner. Also, the owner of the BYOD is prohibited from altering or removing this code without the prior written approval of their supervisor. If they do so they are then subject to immediate termination.
- ENTERPRISE reserves the right to audit any BYOD that connects to an enterprise's infrastructure. Refusal to submit to this audit is grounds for the immediate cessation of all access rights, user ids, and passwords including those from directly connected BYODs.
- Before initial use on the enterprise network or related infrastructure, all BYODs must be registered with the manager they report to. That manager should communicate the use of that device to Information Technology which maintains a list of approved devices, whitelisted wireless networks, related software applications, and utilities. Devices that are not on this list may not be connected to the enterprise's infrastructure.
- End users who wish to connect such devices to non-enterprise network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet the enterprise's established enterprise IT security standards.
- All BYODs attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) can be electronically inspected by ENTERPRISE. Devices that have not been previously approved are not in compliance with ENTERPRISE's security policies or represent any threat to the network or data will not be allowed to connect.
- BYODs may only access the enterprise network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required.

- Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed using procedures approved by or installed by IT.

Security

- Employees using BYODs and related software for network and data access will, without exception, use secure data management procedures.
- BYODs must be protected by a strong password, and all data stored on the device must be encrypted using strong encryption. See ENTERPRISE's password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All users of BYODs must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by ENTERPRISE's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.
- Passwords and other confidential data as defined by ENTERPRISE's IT department are not to be stored unencrypted on BYODs.
- Any BYOD that is being used to store ENTERPRISE data must adhere to the authentication requirements of ENTERPRISE's IT department. Also, all hardware security configurations (personal or company-owned) must be pre-approved by ENTERPRISE's IT department before any enterprise data-carrying device can be connected to it.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with per ENTERPRISE's security policy.
- Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.
- ENTERPRISE reserves the right to remotely wipe or copy any ENTERPRISE data on BYODs that connect or attempt to connect to the network. This includes but is not limited to emails, contacts, business records, financial data, presentations, operational data and metrics, applications, and other data.
- In the event of a lost or stolen BYOD, it is incumbent on the user to report this to IT immediately. The device will be remotely wiped off all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.
- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both corporate-owned and personal mobile devices being used within the company premises.

Device Access Security

- Devices should be locked via a password or biometric device. In the case of an iPhone or iPad, the password should be 4 numbers other than 1234, 0000, 9876, or other sequential combinations. As older devices are replaced biometric security is preferred.

Help & Support

- ENTERPRISE's IT department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused using unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of ENTERPRISE's IT department. This includes, but is not limited to, any reconfiguration of the mobile device.
- IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the enterprise network.

Enterprise Mobile Device Infrastructure

- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.
- The end-user agrees to and accepts that his or her access and/or connection to ENTERPRISE's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains ENTERPRISE's highest priority.
- The end-user agrees to immediately report to his/her manager and ENTERPRISE's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
- Every BYOD user will be entitled to a training session around this policy.
- A BYOD user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

BYOD Infrastructure

- In all cases, all data, applications, user ids, passwords, and sensitive information will remain the property of ENTERPRISE.
- The employee will comply with all backup, record retention, security, sensitive information, business continuity policies, and procedures of ENTERPRISE.
- Under no condition shall any individual (especially children) utilize any BYOD or another device that contains ENTERPRISE data.
- When employees are authorized to use their equipment, ENTERPRISE does not assume responsibility for the cost of equipment, repair, or service.
- Upon termination of employment, the individual grants the company the right to physically inspect the device to validate that all company data and intellectual property has been removed.

Disaster Recovery

The individual is responsible for the recovery of the applications and data on the device. The company will provide processes that can be used to restore company data, intellectual property, and applications.

The device is the property of the individual. If it is destroyed, lost, or stolen the individual is responsible for its replacement. The company has the right to create an image backup of the device but is not obliged to do so. The individual is obligated to notify the company when there is a change in the status (destroyed, lost, or stolen) so they can take appropriate action to deactivate the device and remove it from the approved list of devices that can interact with the company's network and data.

Termination

When an employee ends their employment or relationship with the enterprise, an exit process must be followed and the Employee Termination Checklist must be completed by a supervisor or manager to validate that all data, information, user IDs, and passwords are removed from all BYOD devices.

Backups

IT will provide a mechanism for users to back up their personal materials. IT will assist users having problems with backups. However, IT is not responsible for backing up personal data such as music, movies, etc. Backing up personal information is the users' responsibility. The IT group has recommendations on how to best accomplish backups of personal information.

Public cloud backup such as iCloud is prohibited for all company sensitive and confidential information.

Intellectual Property

The intellectual property contained on the personal device should be backed at least weekly and more frequently, such as daily or twice per day, based on the amount of updating that is done via the device. It is recommended that an automated backup tool be used for this. All data backed up to the cloud should be enciphered and password protected with a "strong" password.

Tablet Computer (iPads)

Enterprise fully supports hardware and software problems on tablet computers as configured by IT. To provide this support, users are required to update their tablets as required by the IT department. IT reserves the right to disconnect any BYOD from the enterprise network if policies are not adhered to by users.

Security

All devices should implement security procedures that require passwords or biometric scanning to use devices. Also, this should include activation of the self-destruction of all data if the password is entered in error consecutively 10 times.

The "FIND ME" application on all GPS-enabled devices should be activated.

Supported Problems

IT will support hardware and software problems on tablet computers as configured.

This means we will support the software that comes with the system from IT. IT will not support software that may be added by users such as; iTunes, games, etc.

Internal Network Access

Computers on the enterprise's network must adhere to all IT policies. If you do not meet these policies you can still get Internet access, as allowed by the enterprise, but you will not get access to enterprise servers that host network data storage and enterprise sensitive and confidential information including enterprise email.

Repair Procedure

Some software and hardware problems may require the IT department to wipe out the current installation of the operating system and reload the computer's original configuration. This will result in the loss of data and any programs installed which are not part of the original configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their tablets.

Upgrade Procedure

Upgrades to a new operating system will be applied by removing the existing installation and replacing it with the new operating system. This will result in the loss of data and any programs installed which are not parts of the configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their tablets.

Patching Policy

As with all networked computers, regular patches to the Operating System and other applications will be installed remotely.

The IT department reserves the right to scan BYODs remotely and apply patches as needed.

BYODs missing important patches will be patched.

BYOD Security Best Practices

For BYOD content management including robust security and device management capabilities are the definition of best practices. CIOs and CSOs should implement the following:

Security Controls

- 256-bit AES encryption per file at rest, 30-day rotating encryption key - Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide.
- 256-bit SSL encrypted data transfer - 256-bit SSL Encryption provides an extra layer of protection for our users. This protection can help defend against login and password theft, which is particularly common in today's wireless society.

Remote BYOD Management

- Automatic timed screen log-out on mobile devices
- At least a 4-digit passcode for each device
- Biometrics to identify specific users and tie to access rights
- Immediate access restriction on the device
- Automatic login to end-user accounts which includes the facility to remotely wipe all data and software from the device
- Automatic shutdown and locking of a device after a security breach from a device
- Security breach reporting

Access Management Controls

- Prohibit access to Application / Web User Interface (UI) from the administrative console
- Prohibit access to content (folders and groups) from the administrative console
- Domain Identity Control: SSO - Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple software systems.

Tablet and Smartphone Applications

- Audit trail for discovery –monitored in real time by a dedicated security audit team or altering the software
- All global files should be available to be accessed and managed (add, change, and delete) directly from the central restricted console -- This includes reporting on the access and use of these files by a device including IP addresses and login ids
- Reporting of all mobile device activity based on:
    - Usage statistics are tracked for files, individual users, and groups
    - Downloads, uploads, previews
    - IP Address

Work From Home - Best Practices

There are best practices for WFH users that are recommended by Janco Associates, Inc. They are:

- **Implement Work From Home Backup Processes** – Define procedures for WFH users
- to back up their devices. Include safeguards to be able to recover data that WFH users created or used.
- **Automatic Process to Purge WFH data** - Have processes in place to purge data automatically when a WFH user is terminated or leaves the organization.
- **Backup Frequently** - Mobile Devices are just that so whenever you are at your base back up to your office or home computer. If you have access to the cloud, consider utilizing backup services that reside there.
- **Security Considerations** - Mobile data often is sensitive therefore only utilize solutions that are enciphered and comply with all mandated and enterprise security requirements.
- **Recover from an Alternative Device** - Use another device of the same type and capacity. If you try to restore data over a mobile over what you have and it fails all could be lost. Sometimes a simple copy from A to B will salvage 80 to 90 percent of critical user data.
- **Write Protect Data** - To prevent the accidental destruction of data, mobile storage devices should be mounted as read-only whenever possible before you attempt any recovery operations. SD cards typically have a write-protect switch, which makes it easier to protect them before attempting a recovery operation. Removable USB drives are more difficult since Windows does not have a way to manually mount their file systems as read-only.

  There is a Registry setting that works with Windows XP SP2 and higher; it forces all USB mass-storage devices into read-only mode. First, create a whole new key: ***HKLM\System\CurrentControlSet\Control\StorageDevicePolicies****.*

  Then create a REG_DWORD entry in it called ***WriteProtect.*** *Set it to 1 and you'll be able to read from USB drives but not write to them.*
- **Be patient** - If you're using a program that supports deep scanning at the cost of a slower recovery process, use it. The speed of this type of scan depends on your system's CPU rather than its I/O, as most of the work involves matching file signatures and checking for false positives.
- **Safely Unplug Mobile Devices** – USB devices, memory cards, and sticks generally tolerate immediate removal, but safely eject these devices before removing them. This reduces the possibility that data will be lost.

BYOD Metrics and SLA Agreement

For CIOs and executive management, a balanced scorecard approach for BYOD service levels is an invaluable tool. That approach allows an enterprise to link the application of BYOD technology to enterprise operations using a "cause-and-effect" approach. Some have likened the balanced scorecard to an SLA solution which enables IT and business line managers to think together about what IT can do to support business performance.

Executive management often questions the benefits and risks associated with investments in IT and BYOD in particular. Below is a list of questions that executive management, business unit executives, and the IT organization as a whole have.

Executive management

- Does IT support the achievement of business objectives?
- What value does the expenditure on IT deliver?
- Are IT costs being managed effectively?
- Are IT risks being identified and managed?
- Are targeted intercompany IT synergies being achieved?

Business unit executives

- Are IT services delivered at a competitive cost?
- Does IT deliver on its service-level commitments?
- Do IT investments positively affect business productivity or customer experience?
- Does IT contribute to the achievement of our business strategies?
- Corporate compliance internal audit
- Are the organization's assets and operations protected?
- Are the key business and technology risks being managed?
- Are proper processes, practices, and controls in place?

IT organization

- Does the enterprise develop the professional competencies needed for successful timely service delivery?
- Are we creating a positive work environment?
- Do we effectively measure and reward individual and team performance?
- Do we capture organizational knowledge to continuously improve performance?
- Can we attract/retain the talent we need to support the business?

To that end, a balanced scorecard can be used to create an effective SLA agreement between IT and the enterprise. An example of specific metrics is shown in the table that follows.

Component	SLA Metric
Customer Satisfaction	• Percentage of customers satisfied with the responsiveness • Percentage of customers satisfied with the cooperation • Percentage of customers satisfied with communication with service support staff
Internal Infrastructure	• Number of problems with BYOD devices and/or services • Number of employees with BYOD • Number of employees using enterprise BYOD devices • Percentage of BYOD meeting information security compliance requirements • Percentage of BYOD meeting records management needs • Staff retention • Staff training as a percentage of revenue
Quality of Information	• The range of information available on BYOD • Percentage of employees using BYOD effectively • Employee satisfaction with the quality of work infrastructure • Percentage of employees satisfied with BYOD quality and scope of information
Financial Performance	• Cost per employee to support BYOD • Cost avoidance due to BYOD • ROI and productivity improvements due to BYOD • Percentage over/under IT budget • IT Budget as a percentage of revenue

Framework for a Balanced Scorecard for a BYOD SLA

A beneficial side effect of the use of the balanced scorecard is that, when all measures are reported, one can calculate the strength of relations between the various value drivers. For example, the relationship between BYOD usage and cost levels might infer that the usage of BYOD does not sufficiently contribute to results as expressed by the other (e.g., financial) performance measures.

Legal Considerations

Privacy

One of the primary privacy considerations in a BYOD policy is the Stored Communications Act (SCA) which was enacted as part of the Electronic Communications Privacy Act (ECPA). The Stored Communications Act is outdated as its authors never contemplated the prevalence of social media and the BYOD (Bring Your Own Device) computing environment.

The SCA deals with the voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" retained by third-party internet service providers (ISPs). Also, it prohibits ISPs from divulging the contents of electronic communications carried, stored, or maintained by the service.

The Stored Communications Act (SCA) makes it an offense for a person or entity to intentionally access without authorization a facility that provides electronic communications service. It is also illegal to intentionally exceed authorization to access such a facility. The person or entity that obtains alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage can be fined or imprisoned. The person whose site has been violated can also seek a civil remedy for the offense.

The risk to employers who obtain unauthorized access to an employee's private site first gained attention in 2009 with the *Pietryllo v. Hillstone Restaurant Group, d/b/a Houston's case*. The company's managers violated the SCA when they did not have authority from the site owners (the employees) to enter the site. The court also found that the managers invaded the privacy of the employees.

An SCA offense may also apply to unauthorized access to a member's private site or group. So the message for every company is not to try to gain unauthorized access to an employee's or member's private site(s) or group(s). Also, do not ask an employee to provide you with the login codes or passwords to access any private sites. Even if the employee provides the information freely as in the *Pietryllo v. Hillstone* case, the employer has to show that the employee was not coerced or threatened to comply with your request.

Companies don't have to stop monitoring because of the Stored Communications Act; they just have to be smart about it. If you ask the owner or administrator for access to a private site and they say no, walk away. Recognize the limitations imposed by employment and privacy laws on your ability to monitor employee sites.

Record Retention

Record Retention - Federal and State Requirements

Under Federal Rule 26(b)(2)(B), parties need not provide discovery of electronically stored information from sources that are not reasonably accessible because of undue burden or cost unless the discovering party establishes good cause for the need for such information. The party asserting undue burden or cost must still identify the sources of information that are not reasonably accessible. Even if a party is excused from searching for and producing records that would be burdensome to produce, the party is not necessarily excused from its obligation to preserve such evidence, as discussed below. It should be noted that even if production is unduly burdensome or costly, the court may still require production if the requesting party establishes a good cause.

The courts look to the reasonableness of a document retention policy. If the policy serves the legitimate business interests of an enterprise, complies with applicable statutory and regulatory requirements, is uniformly applied, and serves to preserve records that may be relevant to a claim or defense involved in threatened or pending litigation, there is little risk of court-imposed sanctions. By following the common-sense measures recommended the organization reduces its risk of legal sanctions and will be able to promptly and properly respond to discovery in the event of litigation or non-compliance during an audit.

Implications Sarbanes-Oxley and Gramm-Leach-Bliley

A business record is essentially any material that contains information about your company's plans, results, policies, or performance. In other words, anything about your company that can be represented with words or numbers can be considered a business record – and you are now expected to retain and manage every one of those records, for several years or even permanently depending on the nature of the information. The need to manage potentially millions of records each year creates many new challenges for your business, especially for your IT managers who must come up with rock-solid solutions to securely store and manage all this data.

Section 802 makes it a crime for anyone to intentionally destroy, alter, mutilate, conceal cover, or falsify any records documents, or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing. Section 802 underscores the importance of record retention and destruction policies that affect all of the company's Email, Email attachments, and documents retained on computers – e-data – as well as hard copies of all company records.

The rules state that if you know your company is under investigation, or even suspect that it might be, all document destruction and alteration must stop immediately. And, you must create company records showing that you've ordered a halt to all automatic e-data destruction practices. Institutions also need to consider all other regulatory rules governing records retention within their industry. For example, for FFIEC, SEC, IRS, etc…most documents must be retained for 7 years.

Security Requirements

Minimum-security requirements for all information and data that affect the financial reporting of ENTERPRISE include at least the following.

- ***Data Security*** – Have a defined set of business and technical rules that clearly state what is expected with data that is captured and used by ENTERPRISE, customers, vendors, and all potentially interested outside parties.
- ***Organizational Security*** – Have a defined set of security guidelines within ENTERPRISE and ENTERPRISE's data that is accessed or processed externally.
- ***Asset Inventory*** – Have an inventory of all assets and established levels of security controls and protection commensurate with the impact of the assets on the books and records of ENTERPRISE.
- ***Procedural Standards*** – Document and communicate the procedures that must be followed daily, weekly, monthly, accounting period, and annually. Included are the processes to monitor the compliance and enforcement of the procedures.
- ***Physical and Environmental Security*** – Have a clear definition of the areas and access points to all assets and data that impact any of the items that are recorded in the "books and records" of ENTERPRISE.
- ***Operations and Communication Security*** – Have processes in place to ensure the security of the dissemination of information, including retrieval, input, modification, backup, and destruction through networks, software, hardware, and physical copies.
- ***Access Control*** – Have a process in place a process for controlling physical and electronic access. This includes protecting all access to the system by unauthorized individuals internal and external to ENTERPRISE.
- ***System Development, Operation, and Maintenance*** – Have processes in place that ensure the system of internal controls is in place, including checks and balances that will negate the possibility of "backdoors" and other unauthorized access to ENTERPRISE's assets, information, systems, and data.
- ***Business Continuity and Disaster Recovery*** – Have processes in place to ensure the survivability of the ENTERPRISE in face of major disruptions of its operations (see https://ww.e-janco.com/drp.htm).
- ***Compliance*** – Have processes in place to validate compliance with the Security Standard including auditing, monitoring, and maintenance of the standards. These processes should include methods for prevention, detection, and correction of defects to the compliance processes.

Appendix

BYOD Policy Decision Table

Device Choice

- Analyzing employee preferences and understanding which devices they have already bought
- Defining an acceptable baseline of what security and supportability features a bring-your-own-device program should support
- Understanding the operating system, hardware, and regional variances around that baseline
- Developing a light-touch certification plan for the evaluation of future devices
- Establishing clear communication to users about which devices are allowed or not, and why
- Ensuring the IT team has the bandwidth

User Experience and Privacy

- Identifying the activities and data IT will monitor
- Clarifying the actions IT will take and under which circumstances
- Defining the BYOD privacy policy
- Critically assessing security policies and restrictions for sustainability
- Deploying core services (email, critical apps, WLAN access) to the employee
- Preserving the native experience
- Communicating compliance issues clearly to the employee

Trust Model

- Identifying and assessing risk for common security posture issues on personal devices
- Defining remediation options (notification, access control, quarantine, selective wipe)
- Setting tiered policy
- Establishing the identity of the user and device
- Lending a critical eye to the sustainability of the security policy being instituted

App Design and Governance

- Designing mobile apps to match the trust level of personal devices
- Modifying app catalog availability based on device ownership
- Committing to the resource investment of building apps with personal devices in mind
- Updating app acceptable-use policies
- Defining enforcement levels for app violations (notification, access control, quarantine, or destruction

Liability

- Defining the elements of baseline protection for enterprise data on BYOD devices
- Assessing liability for personal web and app usage
- Assessing liability for usage onsite vs. offsite, and inside work hours vs. outside work hours
- Evaluating whether the nature of BYOD reimbursement affects liability (partial stipend vs. full payment of service costs)
- Quantifying the monitoring, enforcement, and audit costs of the BYOD compliance policy
- Assessing the risk and resulting liability of accessing and damaging personal data (for example, doing a full instead of a selective wipe by mistake)

Economics

- Shifting the cost of device hardware to the user and moving to a stipend model
- Controlling excess service charges through more responsible usage
- Establishing appropriate service plans, realizing some negotiating leverage might be lost
- Assessing the productivity impact of users being able to use their desired platforms
- Changing the help desk model (with BYOD, employees use the help desk as the last resort instead of a first resort)
- Reducing compliance and audit costs, if the legal assessment shows lower liability with personal devices)
- Assessing tax Implications

Sustainability

- Securing corporate data
- Minimizing the cost of implementation and enforcement
- Preserving the native user experience
- Staying up to date with user preferences and technology innovations

Internal Marketing

- Communicating why the company is moving to BYOD
- Understanding BYOD is an HR initiative as much as an IT initiative
- Defining IT's "brand"
- Supporting the brand message with the appropriate action(s)

Electronic Forms

Eight (8) Electronic forms are included with this policy template. They come separately in their directory.

- BYOD Access and Use Agreement Form
- Employee Termination Checklist
- Mobile Device Security Access and Use Agreement Form
- Mobile Device Security and Compliance Checklist
- Telecommuting IT Checklist
- Telecommuting Work Agreement
- Work From Home IT Checklist
- Work From Home Work Agreement

IT Job Descriptions

Four (4) detailed job descriptions are included with this policy template. They come separately in their directory.

- BYOD Support Specialist
- BYOD Support Supervisor
- Manager BYOD Support
- Manager WFH Support

What's New

2023 Edition

- Termination/end of relationship process added to the policy
  - Added Employee Termination Checklist
- Updated all included forms
- Updated all included job descriptions

2022 Edition

- Updated all included forms
- Updated all included job descriptions

2021 Edition

- Added Work From Home Best Practices
- Added four (4) electronic forms:
  - Telecommuting IT Checklist
  - Telecommuting Work Agreement
  - Work From Home IT Checklist
  - Work From Home Work Agreement
- Added a job description for Manager WFH Support
- Updated all included forms
- Updated all included job descriptions

2020 Edition

- Update section on device ownership options
- Updated all electronic forms
- Updated all attached job descriptions
- Updated all the included procedures to meet compliance mandates

Mobile Device Access & Use Policy

Janco Associates, Inc.

2023 Edition

License Conditions

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the right to use it for a SINGLE enterprise in a single county unless they have a multi-use license. Anyone who makes copies of or uses the template or any derivative of it violates the United States and international copyright laws and is subject to fines that are treble damages as determined by the courts. A REWARD of up to 1/3 of those fines will be anyone reporting such a violation upon the successful prosecution of such violators.

The purchaser agrees that any derivative of this template will contain the following words within the first five pages of that document. The words are:

Published by: **Janco Associates Inc.**
Park City, UT 84060

Email – support@e-janco.com

The publisher cannot in any way guarantee the procedures and approaches presented in this book are being used for the purposes intended and therefore assumes no responsibility for their proper and correct use. Also, we are not attorneys and are not providing a legal opinion as to the data that should be retained for the periods that the data should be retained. The user should check with their legal counsel to determine the specific requirements for record retention and destruction.

Table of Contents

Mobile Access and Use Policy

Overview

Business mobile usage is exploding and becoming an increasingly powerful tool for marketers to connect with consumers around the world. Statistics show that professional text message use is expected to continue growing through the end of this decade. Although few in-depth studies focused on text messaging statistics have been done in the past, recent reports are beginning to shed light on the opportunities and help us grasp the size and potential impact on businesses.

- 5 billion people globally send and receive SMS messages.
- Over 300 million people in North America use text messages
- The mobile industry had a revenue of $2 trillion last year
- 3.3 billion people access the internet via mobile. It's predicted that by 2025, 72.6% of internet users will access the web via mobile-only, using their smartphones.
- 4 billion people are expected to own a smartphone by the end of the decade

The overriding goal of this policy is to protect the Company's technology-based resources (such as corporate data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing corporate technology resources must adhere to company-defined processes for doing so.

The purpose of this policy is to define standards, procedures, and restrictions for end-users who have specific and authorized business requirements to access enterprise data from a mobile device connected via a wireless or unmanaged network outside of ENTERPRISE's direct control. This policy applies to, but is not limited to, all devices and media that fit the following device classifications:

- Smartphones
- PDAs
- USB applications and data
- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Home or personal computers used to access enterprise resources
- BYOD
- Wearable Devices
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

The policy applies to any hardware and related software that could be used to access enterprise resources, even if the equipment is not approved, owned, or supplied by ENTERPRISE.

With the advent of BYOD (Bring Your Own Device) and Wearable Devices, the implications for privacy, security, compliance, and record management are significantly more complex. However, this full policy does apply to those devices as well.

Components of the BYOD Strategy and Basics for BYOD Policy

A BYOD strategy and resultant policy are driven by 8 factors: device choice options; user experience and privacy; internal marketing and training; liability; economics; application design and infrastructure; maintainability; and trust security compliance. Each of these factors has been considered in the creation of this policy. A detailed description of each of these factors is provided later in this policy.

Device Choices

- Analyze employee preferences and understand which devices they already have
- Definite an acceptance baseline of what security and supportability features a bring-your-own-device program should support
- Understand the operating system, hardware, and regional variances around that baseline
- Develop an “easy” certification process for the evaluation of future devices
- Establish clear communication to users about which devices are allowed or not, and why

User Experience and Privacy

- Identify activities and data IT will monitor
- Clarify the actions IT will take and under which circumstances
- Define the BYOD privacy policy
- Access security policies and restrictions for sustainability
- Deploy core services (email, critical apps, WLAN access) to the BYOD
- Preserving the native experience – do not force legacy application structure on BYOD

Trust Security Compliance

- Identify and assess the risk associated with security issues on BYOD
- Identify and define remediation options (notification, access control, quarantine, selective wipe)
- Set policy based on organizational hierarchy
- Establish a process to identify both the user and device
- Communicating compliance issues clearly to the employee
- Focus on the sustainability of the security policy being instituted

Application Design and Infrastructure

- Design BYOD applications to match the trust level of individual BYOD
- Modify the applications catalog availability based on device ownership
- Commit to the resource investment of building applications with BYOD in mind
- Update the application's acceptable-use policies
- Define enforcement levels for application violations (notification, access control, quarantine, or selective wipe or disable)
- Coordinate data created and modified by the ENTERPRISE records management procedures and processes

Economics

- Shift the cost of device hardware to the user and move to a fixed fee per month paid to the user
- Control excess service charges through managed usage
- Establish service plans with outside entities, realizing some negotiating leverage might be lost
- Assess the productivity impact of users being able to use their desired platforms
- Change the help desk model (with BYOD, employees use the help desk as the last resort instead of a first resort)
- Access compliance and audit costs
- Assess tax implications both to the company and the individual

Liability

- Define the elements of the minimum protection for enterprise data on BYOD devices
- Assess liability for personal web and application usage
- Assess liability for usage onsite vs. offsite, and inside work hours vs. outside work hours
- Evaluate whether the nature of BYOD reimbursement affects liability (partial payment vs. full payment of service costs)
- Plan and budget for monitoring, enforcement, and audit of the BYOD compliance policy
- Assess the risk and resulting liability of accessing and damaging personal data (for example, doing a full wipe instead of a selective wipe by mistake)

Maintainability

- Define patch and version control for both software and firmware
- Securing corporate data and meeting ongoing mandated compliance requirements
- Minimize the cost of implementation and enforcement
- Preserve the native user experience
- Stay up-to-date with user preferences and technology innovations

Internal marketing and training

- Communicate why the company is moving to BYOD
- Understand BYOD is an HR initiative as much as an IT initiative
- Define IT's "brand" and level of service to be provided
- Supporting the brand message with the appropriate action
- Develop training materials for both the user and the helpdesk
- Provide 7x24 access to support via the help desk or recommended service providers

Policy

It is the responsibility of any employee, associate, contractor, or others working for or in conjunction with ENTERPRISE who uses a mobile device to access enterprise resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is critical that any mobile device that is used to conduct enterprise business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. If this involves the disclosure or "theft" of information, that action can result in the immediate termination "for cause" of the individuals responsible.

Policy and Appropriate Use

It is the responsibility of any employee of [Company name] who is connecting to the organizational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that every wireless connection used to conduct [Company name] business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- General access to the organizational network through the Internet by residential remote users, including Work From Home (WFH) through the company's network, is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through company networks do not violate any of the company's Internet-acceptable use policies.
- Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key-encrypted strong passwords following the company's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All remote computer equipment and devices used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Users are expected to secure their corporate-connected machines when they are physically on their machines, as well as when they step away. Computers will have installed whatever antivirus software is deemed necessary by the company's IT department. Antivirus signature files must be updated following the existing company policy.
- Due to the potential for bandwidth conflicts within the corporate campus, the use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you need to use such equipment – for example, a wireless phone – please consult IT before proceeding further.
- Before initial use for connecting to the corporate network, all public hotspots must be registered with IT. A list of approved hotspot sites is available for viewing at [Web address.] If your preferred site does not appear on this list, contact the Helpdesk at [e-mail address] or [phone number] to have it registered and added to the list.

- Remote users using public hotspots for wireless Internet access must employ for their devices a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with the company's additional security measures. IT will support its sanctioned hardware and software but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.
- Hotspot and remote users must disconnect wireless cards when not in use to mitigate attacks by hackers and eavesdroppers.
- Users must apply new passwords for every business/personal trip where company data is being utilized over a hotspot wireless service, or when a company device is used for personal Web browsing.
- Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access the company's resources must adhere to the authentication requirements of the company's IT department. Also, all hardware security configurations (personal or company-owned) must be approved by the company's IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed wireless hardware or software without the express approval of the company's IT department. This includes, but is not limited to, split tunneling, dual-homing, non-standard hardware, or security configurations, [add any modification types, as appropriate], etc.
- Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to the company's network via remote access.
- All connections that make use of wireless access must include a “time-out” system. Following the company's security policies, sessions will time out after 15 minutes of inactivity and will terminate after 2 hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate to re-enter company networks through a wireless connection.
- The wireless access user agrees to immediately report to his/her manager and the company's IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, and any other related components of the organization’s technology infrastructure.
- The wireless access user also agrees to and accepts that his or her access and/or connection to the company's networks may be monitored to record dates, times, duration of access, data types, and volumes, [add any additional monitored activities, as appropriate], etc., to identify unusual usage patterns or other suspicious activity [add any additional monitored activities, as appropriate]. As with in-house computers, this is done to identify accounts/computers that may have been compromised by external parties.
- Any questions relating to this policy should be directed to the IT department/service desk.
- IT reserves the right to turn off without notice any access port to the network that puts the company’s systems, data, users, and clients at risk.

Mobile Devices

Regardless of whether individuals work on their tablets, PDAs, or SmartPhones (see list above) or are corporate-issued ones, the policy of ENTERPRISE is that these users must follow IT to support the management, tracking, securing, and supporting of these devices, just like they do for any other corporate computing platform.

Specifically, the policies that apply to these types of devices are:

- Comply with security best practices for tablets, including the use of multilevel passwords and device certificates, and the ability to remotely wipe the device if it is lost or stolen.
- Utilize tiered access to network resources to secure critical data and applications.
- Comply with application delivery mechanisms.

Device/Location	Approved	Limitations
Enterprise Device	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not use it for any personal or non-business-related purpose. All data that resides on enterprise devices is (and becomes) the property of the enterprise. All information is confidential and sensitive and should not be distributed outside of the enterprise without the expressed authorization of the enterprise.
Enterprise approved BYOD	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements. This also means that BYOD meets all security and mandated government and industry requirements.	Limit access to the BYOD device to only authorized and approved users. No games or installation of applications that could be the device and the data contained on it at risk.
Enterprise e-mail	Use the enterprise email account to conduct enterprise business. This allows for the device to be backup, comply with the records management retention and destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not conduct any personal business on the enterprise email account. Never open an unknown attachment or reply to anyone unknown to you.
Enterprise Cloud Storage	Use enterprise cloud storage to access enterprise information	Do not store personal information on enterprise cloud storage.
Personal Cloud Storage	For personal use only	Never store enterprise information on personal cloud storage

Policy Definitions

The following are definitions that apply to this policy:

- **WiFi Network** - A connection point that allows two or more computers, to communicate, (enabling file sharing, printer sharing, internet connection, etc.), using standard protocol but without the use of network cabling and typically outside of ENTERPRISE's control
- **Employee** - An employee, contractor, associate, and others who work away from his/her central workplace either at home or another ENTERPRISE-designated or approved remote work location.
- **Telecommuting** - A work arrangement in which supervisors direct or permit employees to perform their usual job duties away from their central workplace, following work agreements.

Access Control

- The CIO and Information Technology group reserve the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the enterprise's systems, data, users, and clients at risk.
- ENTERPRISE reserves the right to audit any device that connects to the enterprise's infrastructure. Refusal to submit to this audit is grounds for the immediate cessation of all access rights, user ids, and passwords including those from directly connected devices.
- Before initial use on the enterprise network or related infrastructure, all mobile devices must be registered with the manager they report to. That manager should communicate the use of that device to Information Technology which maintains a list of approved devices, whitelisted wireless networks, related software applications, and utilities. Devices that are not on this list may not be connected to the enterprise's infrastructure.
- End users who wish to connect such devices to non-enterprise network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet the enterprise's established enterprise IT security standards.

- All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) can be electronically inspected by ENTERPRISE. Devices that have not been previously approved are not in compliance with ENTERPRISE's security policies or represent any threat to the network or data will not be allowed to connect. Laptop computers or personal PCs may only access the enterprise network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required. Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed using procedures approved by or installed by IT.

Federal Trade Commission Mobile Policy Guidelines

The National Telecommunications and Information Agency, within the U.S. Department of Commerce, is working with other stakeholders to develop a code of conduct on mobile application transparency. To the extent that strong privacy codes are developed, the FTC will view adherence to such codes favorably in connection with its law enforcement work.

The FTC recommends that mobile platforms should:

- Provide just-in-time disclosures to mobile users and obtain their affirmative express consent before allowing applications to access sensitive content like geolocation;
- Provide just-in-time disclosures and obtain affirmative express consent for other content that mobile users would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content;
- Implement a one-stop "dashboard" application approach to allow mobile users to review the types of content accessed by the applications they have downloaded;
- Implement an icon to depict the transmission of user data;
- Promote application developer best practices. For example, platforms can require developers to make privacy disclosures, reasonably enforce these requirements, and educate application developers;
- Provide mobile users with clear disclosures about the extent to which platforms review applications before making them available for download in the application stores and conduct compliance checks after the applications have been placed in the application stores; and
- Consider offering a Do Not Track (DNT) mechanism for smartphone users. A mobile DNT mechanism, which a majority of the Commission has endorsed, would allow mobile users to choose to prevent tracking by ad networks or other third parties as they navigate among applications on their phones.

The FTC recommends that application developers should:

- Have a privacy policy and make sure it is easily accessible through the application stores;
- Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information (to the extent the platforms have not already provided such disclosures and obtained such consent);

- Improve coordination and communication with networks and other third parties that provide services for applications, such as analytics companies, so the application developers can better understand the software they are using and, in turn, provide accurate disclosures to mobile users. For example, application developers often integrate third-party code to facilitate analytics within an application with little understanding of what information the third party is collecting and how it is being used.
- Consider participating in self-regulatory programs, trade associations, and industry organizations, which can guide how to make uniform, short-form privacy disclosures.

The FTC recommends that advertising networks and other third parties should:

- Communicate with application developers so that the developers can provide truthful disclosures to mobile users;
- Work with platforms to ensure the effective implementation of Do Not Track (DNT) for mobile.

The FTC recommends that application developer trade associations, along with academics, usability experts and privacy researchers can:

- Develop short-form disclosures for application developers;
- Promote standardized application developer privacy policies that will enable mobile users to compare data practices across apps;
- Educate application developers on privacy issues.

Security

Mobile networks should not be considered a replacement for wired networks. They should be seen solely as extensions to the existing wired network, and are to be used for general-purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

The addition of mobile access points within corporate facilities is managed at the sole discretion of IT. Non-sanctioned installations of mobile and wireless equipment or the use of unauthorized equipment are strictly forbidden.

This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

- Employees, suppliers, contractors, partners, customers, and other associates using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password, and all data stored on the device must be encrypted using strong encryption. See ENTERPRISE's password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by ENTERPRISE's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.
- Passwords and other confidential data as defined by ENTERPRISE's IT department are not to be stored unencrypted on mobile devices.
- Any mobile device that is being used to store ENTERPRISE data must adhere to the authentication requirements of ENTERPRISE's IT department. Also, all hardware security configurations (personal or company-owned) must be pre-approved by ENTERPRISE's IT department before any enterprise data-carrying device can be connected to it.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with following ENTERPRISE's overarching security policy.
- Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.
- In the event of a lost or stolen mobile device, it is incumbent on the user to report this to IT immediately. The device will be remotely wiped off all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both corporate-owned and personal mobile devices being used within the company premises.

Help & Support

- ENTERPRISE's IT department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of ENTERPRISE's IT department. This includes, but is not limited to, any reconfiguration of the mobile device.
- IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the enterprise network.

Enterprise Mobile Device Infrastructure

- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end-user agrees to and accepts that his or her access and/or connection to ENTERPRISE's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains ENTERPRISE's highest priority.
- The end-user agrees to immediately report to his/her manager and ENTERPRISE's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
- Every mobile device user will be entitled to a training session around this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

Equipment and Supplies

Normally, ENTERPRISE will provide the equipment and supplies needed by employees to effectively perform their duties. However, where agreements specify, employees may be authorized to use their equipment. In all cases, all data and sensitive information will remain the property of ENTERPRISE.

The employees will comply with all backup, record retention, security, sensitive information, business continuity policies, and procedures of ENTERPRISE.

Under no condition shall any individual (especially children) utilize any computer, USB storage device, PDA, Smartphone, or another device that contains ENTERPRISE data.

Enterprise Owed Equipment

- Authorized use/users – ENTERPRISE-owned equipment may be used only for legitimate business purposes by authorized employees.
- Employees are responsible for protecting ENTERPRISE-owned equipment from theft, damage, and unauthorized use.
- Maintenance – ENTERPRISE-owned equipment used in the normal course of employment will be maintained, serviced, and repaired by ENTERPRISE.
- Transporting/Installing – ENTERPRISE Information Technology employees are responsible for transporting and installing equipment, and for returning it to the central workplace for repairs or service. When this occurs IT employees shall have the right to inspect the location where the equipment is located to see that the location complies with all ENTERPRISE policies.

Employee Owned Equipment

- When employees are authorized to use their equipment, ENTERPRISE does not assume responsibility for the cost of equipment, repair, or service.

Tablet Computer (iPads and Microsoft Surface)

Enterprise fully supports hardware and software problems on tablet computers as configured by IT. To provide this support users are required to update their tablets as required by the IT department. IT reserves the right to disconnect any computer, mobile device, and BYOD from the enterprise network if policies are not adhered to by users.

Backups

IT will provide a mechanism for users to back up their materials. IT will assist users having problems with backups. However, IT is not responsible for backing up personal data such as music, movies, etc. Backing up personal information is the users' responsibility. IT has recommendations on how to best accomplish backups of personal information.

Public cloud backup such as iCloud is prohibited for all company sensitive and confidential information.

Security

All tablets and iPads should implement security procedures that require passwords to use the devices. Also, this should include activation of the self-destruction of all data if the password is entered in error more than 5 times.

The "FIND ME" application on Apple and SmartPhone devices should be activated.

Supported Problems

IT will support hardware and software problems on tablet computers as configured.

This means we will support the software that comes with the system from IT. IT will not support software that may be added by users such as; iTunes, games, etc.

Tablet computers are purchased with basic warranty support. This includes hardware problems such as; hard drive failures, electrical shorts, etc. Accidental damage is also covered; tablet dropped dog chewed power cords, water damage, etc.

The tablets also include 4 years of theft recovery protection. If a tablet is lost, IT can work with the service provider to attempt to locate the missing tablet using applications like Apple's "Find Phone".

Internal Network Access

Computers on the enterprise's network must adhere to all IT policies. If you do not meet these policies you can still get Internet access, as allowed by the enterprise, but you will not get access to enterprise servers that host network data storage and enterprise sensitive and confidential information including enterprise email.

Repair Procedure

Some software and hardware problems may require the IT department to wipe out the current installation of the operating system and reload the computer's original configuration. This will result in the loss of data and any programs installed which are not part of the original configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their tablets.

The enterprise's IT department stocks spare tablet computers that can be made available to users if their tablet needs to have repaired.

Upgrade Procedure

Upgrades to a new operating system will be applied by removing the existing installation and replacing it with the new operating system. This will result in the loss of data and any programs installed which are not parts of the configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their tablets.

Patching Policy

As with all networked computers, regular patches to the Operating System and other applications will be installed remotely.

The IT department scans computers weekly and applies patches as needed.

Machines offline during this scan or machines missing important patches will be patched outside of the regularly scheduled period.

Mobile Device Security Best Practices

Mobile Device Security Best practices

With the move towards more mobile and office site computing users are challenged to keep their BYOD devices safe and secure

- Have a clear definition for ownership of the device, data, cell phone numbers, email addresses to use, email clients, email folders, and applications (i.e., What is the process to follow when an employee leaves the organization) – See Employee Termination Checklist.
- Purchase Android devices only from suppliers who release Android patches quickly.
- Implement the locking feature on all mobile devices
- Utilize applications on the device from the vendor (Apple or Google) application store
- When possible utilize two-factor authentication
- Use device encryption
- Connect to Wi-Fi via a Virtual Private Network (VPN)
- Utilize a Password management system
- Utilize anti-virus software
- Turn off un-used features like connections that are not used
- If you don't use an app, uninstall it.

For mobile content management include robust security and device management capabilities are the definition of best practices. CIOs and CSOs should implement the following:

Security controls

- 256-bit AES encryption per file at rest, 30-day rotating encryption key - Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide.
- 256-bit SSL encrypted data transfer - 256-bit SSL Encryption provides an extra layer of protection for our users. This protection can help defend against login and password theft, which is particularly common in today's wireless society. The secondary benefit of 256-Bit SSL Encryption is to help to overcome the speed issues related to ISP throttling and bottlenecks. Most ISPs do not want to throttle or bottleneck 256-Bit SSL Encrypted data because this kind of data is routinely used to send sensitive data (financial information, logins, passwords, credit card info, etc).
- SAS 70 Type II certified, redundant data centers and DR policy - a SAS 70 Type II audit report provides independent 3rd party verification that a service organization’s policies and procedures are correctly designed at a point in time and are operating effectively enough throughout the period (typically 6 months to 1 year) to achieve the specified control objectives.

- 99.9% SLA Uptime Guarantee

Remote device management

- Automatic timed screen log-out on mobile devices
- A 4-digit passcode for each device (at least)
- Immediate access restriction on the device
- Automatic login to end-user accounts which includes the facility to remotely wipe all data and software from the device
- Automatic shutdown and locking of a device after a security breach from a device
- Security breach reporting

Access management controls

- Prohibit access to Application / Web User Interface (UI) from the administrative console
- Prohibit access to content (folders and groups) from the administrative console
- Domain Identity Control: SSO - Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple software systems.

Tablet and Smartphone applications

- Audit trail for discovery – This should be implemented and monitored in real time with a dedicated security audit team or without altering software
- All global files should be available to be accessed and managed (add, change, and delete) directly from a central restricted console -- This includes reporting on the access and use of these files by a device including IP addresses and login ids
- Reporting of all mobile device activity based on:
    - Usage statistics are tracked for files, individual users, and groups
    - Downloads, uploads, previews
    - IP Address

Appendix

Electronic Forms

Nine (9) electronic forms are included with this policy template. They come separately in their directory.

- BYOD Access and Use Agreement Form
- Company Asset Employee Contol Log
- Employee Termination Checklist
- Mobile Device Security Access and Use Agreement Form
- Mobile Device Security and Compliance Checklist
- Wearable Device Access and Use Agreement
- Work From Home Contact Information
- Work From Home IT Checklist
- Work From Home Work Agreement

What's New

2023 Edition

- Updated all attached forms
- Updated Employee Termination Checklist
- Updated to reflect changes due to the remote workforce
- Defined mobile device, BYOD, and Cloud uses and limitations

2022 Edition

- Updated all attached forms
- Added Employee Termination Checklist
- Updated to reflect changes due to the remote workforce
- Define ownership rules

2021 Edition

- Updated all attached forms
- Updated to reflect WFH
- Added four (4) forms
    - Wearable Device Access and Use Agreement
    - Work From Home Contact Information
    - Work From Home IT Checklist
    - Work From Home Work Agreement

2020 Edition

- Updated all the forms to the latest version which meets all mandated security and privacy requirements
- Updated to meet CCPA mandates

Privacy Compliance Policy

Janco Associates

2023 Edition

Conditions

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the right to use it for a SINGLE Disaster Recovery Plan unless the user has purchased a multi-user license. Anyone who makes an unlicensed copy of or uses the template or any derivative of it violates the United States and international copyright laws and is subject to fines that are treble damages as determined by the courts. A REWARD of up to 1/3 of those fines will be paid to anyone reporting such a violation upon the successful prosecution of such violators.

The purchaser agrees that any derivative of this template will contain the following words within the first five pages of that document. The words are © Copyright Janco Associates, Inc. – ALL RIGHTS RESERVED

NOTE: We are not attorneys, nor do we purport to provide any legal advice. It is up to the reader to validate and requirements, procedures, and processes that are mandated by the laws described here with their attorneys.

Also, the reader cannot assume that we have presented all the privacy mandates. If you should find some additional requirements please forward a note to support@e-janco.com.

Table of Contents

Privacy Compliance Policy – U.S. and EU Mandated Requirements

Overview

Mandated privacy requirements are designed to protect the individual's privacy from unwarranted invasion, to make sure that personal information in possession of an entity is properly used, and to prevent any potential misuse of personal information in the possession of that entity. This policy establishes the processes and procedures, and assigns responsibilities, for fulfilling mandated privacy requirements.

The Chief Security Officer or delegate must approve all processing activities at ENTERPRISE associated with information (data) that falls within mandated privacy requirements. This information includes but is not limited to customer identification data, contact information, email addresses, social security numbers, credit card numbers, credit card expiration dates, security codes, passwords, customer names, customer numbers, ENTERPRISE proprietary data, and any other data (i.e. California Personal ID number).

This policy applies to the entire enterprise, its vendors, its suppliers (including outsourcers), and co-location providers and facilities regardless of the methods used to store and retrieve this information (e.g. online processing, outsourced to a third party, Internet, Intranet, or swipe terminals).

All processing, storage, and retrieval activities for this information must maintain strict access control standards and the Chief Security Officer mandates these specific policies be followed.

Right to Privacy

Right to privacy has been defined in two major pieces of legislation – one for the EU (GDPR) and the other in the California Privacy Act:

- The right to know what personal information is being collected about them.
- The right to know whether their personal information is sold or disclosed and to whom.
- The right to say no to the sale of personal information.
- The right to access their personal information.
- The right to equal service and price, even if they exercise their privacy rights.

The definition of the specifics of the legislation and policies necessary to comply follows. All individuals capturing, viewing, or using consumer data need to follow the rules and guidelines to meet the Privacy Compliance Mandates.

California Consumer Privacy Act

Under the California Consumer Privacy Act, the following set of privacy requirements are mandated: and policies are to be followed.

Consumer's Right to Know Information that Has Been Captured

1. A consumer shall have the right to request that an Enterprise that collects a consumer's personal information disclosed to that consumer the categories and specific pieces of personal information the business has collected.
2. An Enterprise that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. An Enterprise shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.
3. An Enterprise shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.
4. An Enterprise that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, a readily useable format that allows the consumer to transmit this information to another entity without hindrance. An Enterprise may provide personal information to a consumer at any time but shall not be required to provide personal information to a consumer more than twice in 12 months.
5. This section shall not require An Enterprise to retain any personal information collected for a single, one-time transaction if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.
   (1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.
   (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

Consumer's Right to Have Data Removed

1. A consumer shall have the right to request that An Enterprise delete any personal information about the consumer that the business has collected from the consumer.
2. An Enterprise that collects personal information about consumers shall disclose the consumer's rights to request the deletion of the consumer's personal information.
3. An Enterprise that receives a verifiable request from a consumer to delete the consumer's personal information according to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.
4. An Enterprise or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information to:
   (1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of An Enterprise's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
   (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
   (3) Debug to identify and repair errors that impair existing intended functionality.
   (4) Exercise free speech - ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
   (5) Comply with the California Electronic Communications Privacy Act pursuant.
   (6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research if the consumer has provided informed consent.
   (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
   (8) Comply with a legal obligation.
   (9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Consumer's Right to Know How Data is Used

1. A consumer shall have the right to request that An Enterprise that collects personal information about the consumer disclose to the consumer the following:
   (1) The categories of personal information have been collected about that consumer.
   (2) The categories of sources from which personal information is collected.
   (3) The business or commercial purpose for collecting or selling personal information.
   (4) The categories of third parties with whom the business shares personal information.
   (5) The specific pieces of personal information have been collected about that consumer.
2. An Enterprise that collects personal information about a consumer shall disclose to the consumer, according to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable request from the consumer.
3. An Enterprise that collects personal information about consumers shall disclose:
   (1) The categories of personal information have been collected about that consumer.
   (2) The categories of sources from which personal information is collected.
   (3) The business or commercial purpose for collecting or selling personal information.
   (4) The categories of third parties with whom the business shares personal information.
   (5) The specific pieces of personal information the business has collected about that consumer.

Consumer's Rights to Data That is Sold

1. A consumer shall have the right to request that An Enterprise that sells the consumer's personal information, or that discloses it for An Enterprise purpose, disclose to that consumer:
   (1) The categories of personal information that the business collected about the consumer.
   (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
   (3) The categories of personal information that the business disclosed about the consumer for An Enterprise purpose.
2. An Enterprise that sells personal information about a consumer, or that discloses a consumer's personal information for An Enterprise purpose, shall disclose to the consumer upon receipt of a verifiable request from the consumer.
3. An Enterprise that sells consumers' personal information, or that discloses consumers' personal information for An Enterprise purpose, shall disclose:
   (1) The category or categories of consumers' personal information has been sold, or if the business has not sold consumers' personal information, it shall disclose that fact.
   (2) The category or categories of consumers' personal information has been disclosed for An Enterprise purpose, or if the business has not disclosed the consumers' personal information for An Enterprise purpose, it shall disclose that fact.
4. A third party shall not sell personal information about a consumer that has been sold to the third party by An Enterprise unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.

Consumer's Rights for Stopping the Sale of Data

1. A consumer shall have the right, at any time, to direct An Enterprise that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out.
2. An Enterprise that sells consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the right to opt out of the sale of their personal information.
3. An Enterprise that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.
4. An Enterprise shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. An Enterprise that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

Consumer's Rights to Not be Discriminated Due to Opt-Out

1. An Enterprise shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to:
    (1) Denying goods or services to the consumer.
    (2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
    (3) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights.
    (4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
2. Nothing prohibits An Enterprise from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer if that difference is reasonably related to the value provided to the consumer by the consumer's data.
3. An Enterprise may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. An Enterprise may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

   An Enterprise that offers any financial incentives shall notify consumers of the financial incentives.
4. An Enterprise may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.
5. An Enterprise shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious.

Enterprise Reporting Requirements

In a form that is reasonably accessible to consumers, An Enterprise shall:

1. Make available to consumers two or more designated methods for submitting requests for information required to be disclosed, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.
2. Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is verifiable, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12 months preceding the business's receipt of the verifiable request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business to make a verifiable request.
    (1) To identify the consumer, associate the information provided by the consumer in the verifiable request with any personal information previously collected by the business about the consumer.
    (2) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories that most closely describes the personal information collected.
3. Identify the consumer and associate the information provided by the consumer in the verifiable request with any personal information previously collected by the business about the consumer.
4. Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold.
5. Identify by category or categories the personal information of the consumer that the business disclosed for An Enterprise purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for An Enterprise purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list
6. Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:
    (1) A description of a consumer's rights and one or more designated methods for submitting requests.
    (2) A list of the categories of personal information has been collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

7. Provide two separate lists:
    (1) A list of the categories of personal information has been sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.
    (2) A list of the categories of personal information has been disclosed about consumers for An Enterprise purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for An Enterprise purpose in the preceding 12 months, the business shall disclose that fact.
8. Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements and how to direct consumers to exercise their rights under those sections.
9. Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for verification.
10. An Enterprise is not obligated to provide the information to the same consumer more than twice in 12 months.

Enterprise Internet and WWW requirements

An Enterprise that is required to comply in a form that is reasonably accessible to consumers

1. Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. An Enterprise shall not require a consumer to create an account to direct the business not to sell the consumer's personal information.
2. Include a description of a consumer's rights along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:
    (1) Its online privacy policy or policies if the business has an online privacy policy or policies.
    (2) Any California-specific description of consumers' privacy rights.
3. Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements and how to direct consumers to exercise their rights under those sections.
4. Consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.
5. For a consumer who has opted out of the sale of the consumer's personal information, respect the consumer's decision to opt out for at least 12 months before requesting that the consumer authorized the sale of the consumer's personal information.
6. Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely to comply with the opt-out request.
7. Nothing shall be construed to require An Enterprise to comply with the title by including the required links and text on the homepage that the business makes available to the public generally if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.
8. A consumer may authorize another person solely to opt out of the sale of the consumer's personal information on the consumer's behalf, and An Enterprise shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, according to regulations adopted by the Attorney General.

GDPR

The General Data Protection Regulation (GDPR) sets specific compliance requirements on how your business does business with enterprises and individuals in the EU.

The EU requires that enterprises need to have consent or legitimate interests to use personal data. Whether you rely on consent or legitimate interests for your marketing, you need to do similar things to make sure you are GDPR compliant:

- ❑ Be clear with individuals about why you need their data at the point of collection
- ❑ Always use clear and concise language appropriate for your target audience
- ❑ Provide information at the point the data is collected. It cannot be hidden in small print.
- ❑ Give individuals control over their data. They should be able to decide whether to share their data with you or not.
- ❑ Under the GDPR principle of accountability, you should be able to demonstrate that you are compliant. This means recording the legal grounds for processing an individual's data.

Why Data is Captured

- ❑ To capture personal data the enterprise needs to demonstrate that they have a valid business or marketing reason to capture and retain data on an individual
- ❑ Validated that legitimate interests are the most appropriate lawful basis for processing
- ❑ Communicate how or why there is a need for an individual's data when it is collected
- ❑ Utilize a layered privacy notice/policy - A layered privacy notice puts the most important information upfront and then there is a more detailed privacy policy underneath it
- ❑ Inform Individuals on what the plan is for their data when it is collected
- ❑ Allow individuals to "opt-out" of marketing
- ❑ Collect the minimum data necessary and delete records after use
    - Data needed for a suppression file can be kept.
    - Have a valid reason to process an individual's data using your legal legitimate interests. For example, an individual may have acquired a product, therefore, the business can market similar products to the customer

User Consent

Consent needs are positively given. That process needs to be documented

Asking for Consent

- ❑ Validate that consent is the most appropriate lawful basis for processing
- ❑ Ask for consent prominently and separately from our terms and conditions
- ❑ Implement a positive "opt-in"
  - Do not use pre-ticked boxes or any other type of consent by default
  - Utilize plain easy to understanding the language
- ❑ Explain why the data is needed and what we're going to do with it
- ❑ Provide specific options for consent for the different types of data processing we carry out
- ❑ Identify your organization and third parties the data may be shared with
- ❑ Inform the individual they can withdraw consent at any time
- ❑ Inform the individual they can refuse to consent without detriment
- ❑ Do not make consent a precondition of our service
- ❑ If we offer online services to children, we ask for consent after we have completed age verification and have parental consent measures in place

Recording consent

- ❑ Keep a record of when and how consent was obtained from the individual
- ❑ Keep a record of exactly what they were told at the time

Managing consent

- ❑ Regularly review consent to make sure that the relationship, the processing, and the purposes have not changed since consent was given
- ❑ Have the means to refresh consent at appropriate intervals, including any parental consent
- ❑ Using privacy dashboards or other preference-management tools is good practice
- ❑ Make it easy for individuals to withdraw their consent at any time, and show them how to do so
- ❑ When consent is withdrawn, act as soon as we can
- ❑ Do not penalize individuals who want to withdraw their consent

Communication

When collecting personal data, you will need to make sure individuals are aware of the following:

- ❑ The identity and contact details of the organization
- ❑ Contact details of the data protection officer, if you have one (see Data Protection Officer job description - https://www.e-janco.com/Data-Protection-Officer-Job-Description.html
- ❑ The consent or legitimate interests necessary for data processing and why If the organization uses legitimate interests, legal grounds to contact individuals then this must be explained
- ❑ Which third parties that personal data may be passed to
- ❑ In other countries outside the EU, the data may be processed
- ❑ How long the data will be stored, if that is not possible, then the criteria used to determine that period
- ❑ Inform individuals about their right to have their data deleted or redacted, and to object to data processing in the future
- ❑ The right to complain to the national data protection authority, which is the Information Commissioner's Office (ICO)
- ❑ If a statutory or contractual law requires an individual's data
- ❑ Information about automated decision-making, including profiling. Organizations should explain, “Meaningful information about the logic involved” in profiling.

Third-Party Data

When buying third-party data, utilize due diligence. The GDPR makes you accountable and responsible for making sure the personal data you use for marketing is compliant. To be sure, give third-party data suppliers rigorous checks. You should:

- ❑ Know how the list was compiled - If an organization withholds this information then do not use them
- ❑ Know whether the consent was recently obtained/updated
- ❑ Make sure that the third party can prove consent
- ❑ Ask whether data has been screened against the Telephone Preference Service and/or Mailing Preference Service. If not, you will need to screen the data.
- ❑ Make sure your organization is specially named when the data was collected - This may be a requirement in the ICO’s consent guidance so think about how you would manage it.
- ❑ See a sample of the data

Record this process so you have proof that you’ve carried out extensive due diligence on your third-party data suppliers.

Profiling

Profiling means evaluating personal data so you can make predictions about an individual or group. Marketing communications can then be targeted and personalized for individuals or groups.

- ❑ Tell people how and why we prole personal data but give people the chance to opt-out
- ❑ Explain how you prole an individual's data in your privacy notice/policy

If you process personal data via automated decision making then:

- ❑ Consent may need to be explicit - an informed opt-in like a tick box with a clear copy explaining any consequences for individuals

If the profiling has legal or other 'significant effect' on individuals

- ❑ You need explicit consent
- ❑ Undertake a privacy impact assessment to determine whether legitimate interest or consent, is the most appropriate legal basis for your activities

Legacy data

To continue marketing to individuals in your database, you must make sure that data is GDPR compliant. You will have to satisfy the requirements mentioned in the consent, legitimate interests, and information provision sections of this checklist above.

As long as the data you use is GDPR compliant then the ICO will have confirmed that the data can be used after May 2018.

To get your legacy data GDPR compliant:

- ❑ Demonstrate to individuals why you have collected their data
- ❑ Say this in clear and concise language appropriate for your target audience
- ❑ Give individuals the chance to object to the processing of their data
- ❑ Because you should be able to demonstrate compliance with GDPR, you should record your legal grounds for processing an individual's data
- ❑ Demonstrate you have informed the individual what you are doing with their data and why. If cannot demonstrate this, you cannot prove your legacy list is compliant.
- ❑ Reconnect with people in your database using direct mail This is your legitimate interest and does not require consent
- ❑ Renew consent at least every two years once you've reconnected

PCI

The sensitive information policy of ENTERPRISE applies to all system components, which are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The sensitive information PCI DSS policy is that all cardholder data is protected, and cardholder data that is not allowed (see PCI DSS requirements) to be stored is removed from the system once the card has been authorized.

The primary account number, cardholder name, service code, and expiration date can be stored if that data is sufficiently protected as specified in the PCI DSS standard.

The Payment Card Industry Data Security Standard (PCI DSS) requirements apply to all "system components." A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment.

A service provider or merchant may use a third-party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant services of the third party provider must be scrutinized either in 1) each of the third party provider's clients' PCI audits, or 2) the third party provider's PCI audit.

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS

- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by the Internet, wireless, a virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded

Wi-Fi

If Wi-Fi technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a Wi-Fi local area network (LAN) is connected to or part of the cardholder environment (for example, not separated by a firewall), the requirements and testing procedures of PCI for Wi-Fi environments apply. Basic Wi-Fi can be implemented with minimal protection. A company should carefully evaluate the need for the technology against the risk. Consider deploying Wi-Fi technology only for non-sensitive data transmission.

Outsourcing

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance must document the role of each service provider. Additionally, the service providers are responsible for validating their compliance with the PCI DSS requirements, independent of their customers' audits. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to the PCI DSS.

Sampling

To test compliance with the PCI DSS standard ENTERPRISE may select a representative sample of system components to test. The sample must be a representative selection of all the types of system components and include a variety of operating systems, functions, and applications that apply to the area being reviewed. For example, the reviewer could choose Sun servers running Apache WWW, NT servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single OS (for example, NT, Sun), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When selecting samples of merchants' stores or franchised merchants, ENTERPRISE should consider the following:

- If there are standards (required PCI DSS processes in place that each store must follow) the sample can be smaller than is necessary if there are no standard processes, to provide reasonable assurance that each store is configured per the standard process.
- If there is more than one type of standard process in place (for example, for different types of stores), then the sample must be large enough to include stores secured with each type of process.

- If there are no standard PCI DSS processes in place and each store is responsible for its processes, then the sample size must be larger to be assured that each store understands and implements PCI DSS requirements appropriately.

	Data Element	*Storage Permitted*	*Protection Required*	*PCI DSS Requirement 3.4*
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name*	Yes	Yes*	No
	Service Code*	Yes	Yes*	No
	Expiration Date	Yes	Yes*	No
Sensitive Authentication Data**	Full Magnetic Stripe	No	N/A	N/A
	CVC2/CVV2/CID	No	N/A	N/A
	Pin / Pin Block	No	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during the business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored after authorization (even if encrypted).

The PCI DSS requirements[1] are:

- Build and Maintain a Secure Network
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Card Holder Data
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Regularly Monitor and Test Networks
- Requirement 12: Maintain a policy that addresses information security for employees and contractors
- Requirement 13: Hosting providers protect the cardholder data environment

HIPAA

ENTERPRISE may use health information, that is, information that constitutes protected health information as defined in the Privacy Rule of the Administrative Simplification provision of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), for purposes of making or obtaining payment for your care and conducting health care operations. ENTERPRISE has established this policy to guard against unnecessary disclosure of health information.

[1] Attached to this document is a copy of a PCI audit program.

Gramm-Leach-Bliley (Financial Services Modernization Act of 1999

Gramm-Leach-Bliley (GLBA) addresses both information security and privacy and holds ENTERPRISE management accountable to evaluate risks and implement controls to keep all information secure. Features of the act include:

- Financial groups are required by GLBA to notify customers of policies related to disclosing nonpublic customer information to affiliates and third parties.
- Protected information includes:
  - Name
  - Address (Physical and email)
  - Phone number
  - Credit Card numbers
  - Social Security Number
  - Loan application information
  - Credit history
- Customers need to be given the option to opt out of having their private information disclosed.
- Notification should be:
  - At the beginning of the relationship and
  - At least annually to all customers

Massachusetts 201 CMR 17.00 Data Protection Requirements

Standards for the Protection of Personal Information of Residents of the Commonwealth - Organizations that do business with Massachusetts residents must:

- Control passwords to ensure they are kept in a location and/or format which will not compromise the security of the data they protect
- Encrypt all personal information stored on laptops or other portable devices
- Ensure reasonably up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information
- Ensure up-to-date versions of system security agent software, which must include malware protection and up-to-date patches and virus definitions
- Have a Written Information Security Program (WISP) and take "reasonable steps" to ensure that any third-party/independent contractors comply with these data protection provisions. *Note: A copy of the WISP checklist is in the appendix of this template*.

User/Customer Sensitive Information and Privacy Bill of Rights

Users and customers of the enterprise's systems and networks will have the following rights:

- Enterprise will provide Users/customers of the enterprise's systems a privacy policy regarding the data they collect.
- Users/customers of the enterprise's systems have the right to know what type of personally identifiable information is being collected and how long that personally identifiable information is kept by the enterprise and any other related third party.
- Users/customers of the enterprise's systems can expect that an enterprise or related 3rd party that holds their personally identifiable information in connection with a transaction or service is adequately protecting the personally identifiable information from disclosure to unauthorized persons.
- Users/customers of the enterprise's systems will receive notice from an enterprise or related 3rd party, if personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person and could result in identity theft or fraud.
- If a third party has been breached, the enterprise will report that to the enterprise's users/customers.
- Users/customers of the enterprise's systems will receive notice from the enterprise in the event of a data breach, by mail or e-mail, and without "unreasonable delay" (never later than 60 days after a breach, unless a criminal investigation is potentially affected.)
- Service providers that have obtained personally identifiable from the enterprise will send a notification regarding a data breach of protected information that is held by them, under mandated laws such as SOX, PCI, HIPPA, and other mandated requirements.
- Users/customers of the enterprise's systems will receive a general description of the actions taken by the enterprise to restore the security and confidentiality of the personally identifiable information involved in a data breach.
- Users/customers of the enterprise's systems will be provided at least 12 months of identity theft protection at the enterprise's expense.
- Enterprise will notify users/customers of a summary of the breach as victims of identity theft under the Fair Credit Reporting Act.

Appendix

Forms

Attached are forms that are in the subdirectory titled forms

Privacy Compliance Policy Acceptance Agreement

Job Descriptions

Attached are job descriptions which are in the subdirectory titled Job Descriptions

Chief Security Officer

Data Protection Officer

Manager Compliance

Manager Security and Workstations

Security Architect

Privacy and Security Compliance Implementation Work Plan

The privacy and security compliance process to meet the EU's GDPR and California's CCPA is a multi-step process involving both the IT function and the enterprise's operations movement. The focus is on the two prongs of GDPR and CCPA compliance mandates – privacy and security

Define where the enterprise is and the issues it faces.

Define privacy requirements

1. Review existing privacy policies and statements and document how they compare with GDPR and CCPR requirements
2. Assess data subject rights to consent, use, access, correct, delete and transfer personal data
3. Discover and classify personal data assets and affected systems
4. Identify potential access risks

Define security requirements

1. Assess the current state of your security policies, identify gaps, benchmark maturity, and establish conformance roadmaps
2. Identify potential vulnerabilities, supporting security and privacy by design
3. Discover and classify personal data assets and affected systems in preparation for designing security controls

Define what must be done

Document privacy requirements

1. Create a work plan that details your GDPR and CCPR remediation and implementation activities
2. Design the policies, business processes, and supporting technologies you'll need to implement your plans
3. Create a GDPR and CCPR reference architecture
4. Evaluate compliance governance processes

Document security requirements

1. Develop security remediation and implementation plan
2. Define a security reference architecture
3. Define technical and Key Performance Indicators (KPIs) to reduce risk, including encryption, pseudonymization, access control, and monitoring.

Implement changes

Implement privacy requirements

1. Implement and execute policies, processes, and technologies
2. Automate data subject access requests

Implement security requirements

1. Implement privacy-enhancing controls, including encryption, tokenization, and dynamic masking
2. Boost protection by implementing security controls; mitigate access risks and security vulnerabilities

Operate and maintain the new GDPR and CCPA environment

Manage privacy

1. Manage GDPR and CCPA data governance practices, including information lifecycle governance
2. Manage GDPR and CCPA enterprise conformance programs, including those for data use, consent activities, and data subject requests
3. Monitor personal data access
4. Maintain compliance governance process and manage GDPR and CCPA roles and identities
5. Develop GDPR and CCPA KPI metrics and reporting schemas

Manage Security

1. Manage and implement security program practices, including those for risk assessment, roles and responsibilities, and program effectiveness
2. Manage and monitor security operations and intelligence to help detect, respond to and mitigate threats
3. Manage incident response and forensics practices

Govern, audit, and report on compliance

Govern privacy compliance requirements

1. Record personal data access audit trails, including individuals' rights to access, modify, delete and transfer data
2. Perform data processor and controller governance, including providing processor guidance, tracking data processing activities, providing audit trails, and preparing for data subject access requests
3. Document and manage your compliance program, including ongoing monitoring, assessment, evaluation, and reporting of GDPR and CCPA activities
4. Respond to and manage breaches

Govern security compliance requirements

1. Coordinate technical and organizational measures to ensure security appropriate to processing risk
2. Document your security program, including ongoing monitoring, assessment, evaluation, and reporting of security controls and activities
3. Respond to and manage breaches

What's New

2023 Edition

- Updated the User Bill of Rights
- Updated all the attached electronic forms to meet the most current version.
- Updated all the attached job descriptions to meet the latest requirements.

2022 Edition

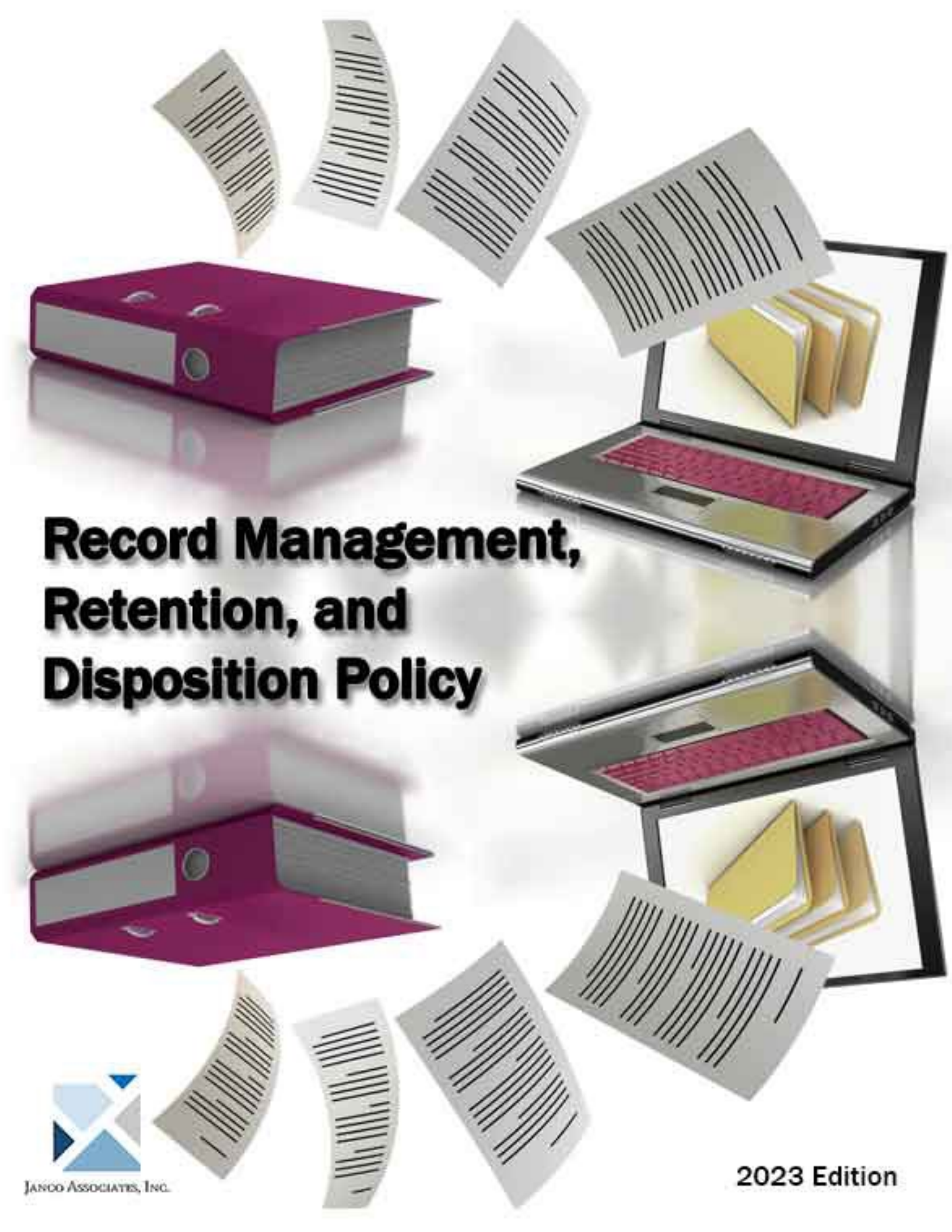
- Updated the User Bill of Rights
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

2021 Edition

- Updated to meet the latest compliance requirements
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

2020 Edition

- Updated to meet the latest compliance requirements
- Updated all the attached electronic forms to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements



Record Management, Retention, and Disposition Policy

Jancoo Associates, Inc.

2023 Edition

License Conditions

Published by: **Janco Associates Inc.**

Park City, UT 84060
Email – support@e-janco.com

The publisher cannot in any way guarantee the procedures and approaches presented in this book are being used for the purposes intended and therefore assumes no responsibility for their proper and correct use. Also, we are not attorneys and are not providing a legal opinion as to the data that should be retained nor the periods that the data should be retained. The user should check with their own legal counsel to determine the specific requirements for record retention and destruction.

Printed in the United States of America

ISBN13 978-1-881218-11-1

Table of Contents

Record Classification, Management, Retention and Disposition Policy Statement

Overview

Data and records that need to be retained are growing at a compound annual growth rate of 60% Data storage and information management costs need to keep up. As data volume and storage infrastructure grow, our company is tasked with meeting our operational service levels and cost containment objectives while also supporting corporate data retention, privacy, and eDiscovery obligations. Close cooperation between legal and IT is crucial to achieving this business' legal, and IT operational objectives.

Contrary to what such decision-makers may think, no organization operating in the United States, regardless of size or industry, is immune from the obligation to retain electronic content following the Federal Rules of Civil Procedure (FRCP).

The FRCP is a body of rules and procedures that govern civil lawsuits in United States district courts. The FRCP creates obligations on the part of all organizations to locate, preserve, and produce, promptly, electronic information relevant to the subject matter of a lawsuit.

The executive management of ENTERPRISE has adopted guidelines to require that each ENTERPRISE unit institute record management, retention, and disposition procedures for the proper management of ENTERPRISE records. Executive management may, from time to time, amend the guidelines as appropriate or as required by law.

Such guidelines shall be consistent with applicable statutes governing the retention of original records and disposition of obsolete records, as well as with any contractual commitments or federal law or regulation which may apply. The guidelines provide for the proper maintenance and protection of archived records, and for the adoption of schedules for the disposition of obsolete records, which schedules shall to the extent practicable given ENTERPRISE needs and requirements be consistent with requirements defined by executive management.

The words "records" means all books, papers, electronic files, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any employee of ENTERPRISE, executive office, department, board, commission, bureau, division or authority of ENTERPRISE.

Compliance with and implementation of the guidelines and any supplementary procedures is the responsibility of all ENTERPRISE employees.

Upon approval of the guidelines or any amendment thereto, the executive management shall forward the guidelines to all ENTERPRISE units. The executive management or its designees shall also establish specifications and timetables for the development of supplementary record classification, management, retention, and disposition procedures and data retention/disposition schedules for ENTERPRISE units. ENTERPRISE unit procedures must adhere to this policy and the published guidelines.

Scope

Compliance with and implementation of the guidelines and any supplementary procedures is the responsibility of all ENTERPRISE employees.

Upon approval of the guidelines or any amendment thereto, the executive management shall forward the guidelines to all ENTERPRISE units. The executive management or its designees shall also establish specifications and timetables for the development of supplementary record classification, management, retention, and disposition procedures and data retention/disposition schedules for ENTERPRISE units. ENTERPRISE unit procedures must adhere to this policy and the published guidelines.

Work From Home impact

Work from Home adds to the complexity of the records management process. All forms of records that are accessed, updated, created, and stored (electronically and physically) need to comply with the records management, retention, and disposition policy of the enterprise. The Manager WFH Support (job description attached) is the focal point for the training of the WFH staff and management of the policy.

What is Record Classification and Management

The foundation of any good record management program is developing a consistent records classification system across the organization.

While there are many record classification systems, one recommended best practice is a three-tier classification based on business function, record class, and record type.

The first step toward developing such a records classification system is taking an inventory or a comprehensive and accurate listing of locations and contents of all records within the organization.

The second step is grouping the records in the inventory according to business functions, record class, and record type:

- ✓ Common business functions include operations, finance, legal, marketing, human resources, and others.
- ✓ The top-level business functions are broken down into record classes. For instance, two record classes of record-function accounting are accounts payable and accounts receivable.
- ✓ Record types are a further subdivision of record classes. For instance, the accounts payable record class can be further broken down into accounts payable aging reports, accounts payable distribution reports, cash disbursement reports, and other categories.

No matter which classification system is adopted, the selected system should address all records regardless of the media type.

The success of a records management program depends on the ease and efficiency of retrieval of the required data. The inability to retrieve the required data on a timely basis causes costly hold-ups, decreases organizational efficiency, degrades organizational quality, and even leads to litigation and fines.

The best practice in this regard is indexing all records, regardless of the media, in a systematic matter with multiple indexing heads. Possible indexing heads include subject matter based on content, subject matter based on context, record creator, intended recipient, date of creation, and others.

The indexing policy needs reinforcement through an access control policy and safeguards. The access policy should define as:

- ✓ The extent of access to records for each employee.
- ✓ An authorization process that includes checks against the laid-down access policy before retrieval of records
- ✓ A means to record and track the retrieval of records

A well-laid-out authorization and access policy help maintain confidentiality and prevents unauthorized disclosure or data theft.

Regulatory Overview

Record Retention - Federal and State Requirements

Under Federal Rule 26(b)(2)(B), parties need not provide discovery of electronically stored information from sources that are not reasonably accessible because of undue burden or cost, unless the discovering party establishes good cause for the need for such information. The party asserting undue burden or cost must still identify the sources of information that are not reasonably accessible. Even if a party is excused from searching for and producing records that would be burdensome to produce, the party is not necessarily excused from its obligation to preserve such evidence, discussed below. It should be noted that even if production is unduly burdensome or costly, the court may still require production if the requesting party establishes a good cause.

The courts look to the reasonableness of a document retention policy. If the policy serves the legitimate business interests of an enterprise, complies with applicable statutory and regulatory requirements, is uniformly applied, and serves to preserve records that may be relevant to a claim or defense involved in threatened or pending litigation, there is little risk of court-imposed sanctions. By following the common-sense measures recommended the organization reduces its risk of legal sanctions and will be able to promptly and properly respond to discovery in the event of litigation or non-compliance during an audit.

Record Retention Implications Sarbanes-Oxley Sections 302, 404, and 409

A record is essentially any material that contains information about your company's plans, results, policies, or performance. In other words, anything about your company that can be represented with words or numbers can be considered a business record – and you are now expected to retain and manage every one of those records, for several years or even permanently depending on the nature of the information. The need to manage potentially millions of records each year creates many new challenges for your business, especially for your IT managers who must come up with rock-solid solutions to securely store and manage all this data.

SOX - Section 302

Section 302 pertains to corporate responsibility for financial reports and requires that the CEO and CFO personally stand behind the accuracy of their company's quarterly and annual financial statements. To do so, senior management needs to be very confident in the financial documentation that is flowing through the company. For the CEO and CFO to certify that the financial statements are correct, systems must be in place to pull together all of the business performance data from all across the company – even if that data resides in various countries, departments, business units, and/or in separate data centers or on different networks.

All of the business information must unite into one comprehensive and accurate financial view of the business. Typically, all of the divisions and departments within a company submit data that is rolled up the ladder to the corporate accounting or controller's office, where the data is further consolidated into a quarterly or annual financial statement awaiting the CFO's sign-off. Several versions of these reports and spreadsheets may flow back and forth as the final numbers are revised. All of these spreadsheets, as well as all of the documents and Emails that were used to arrive at the financial conclusions, are considered records under SOX.

They must all be retained, and they all are auditable. Before the CEO and CFO sign off on the company's financial statements, they need to be sure there is a process in place to manage all the records that were used to generate the financial statements. The CEO and CFO are on the line, and they face severe penalties if serious errors or fraud find their way into the financial reporting and communications about them the CEO and CFO.

SOX - Section 404

Section 404 requires that annual reports contain a discussion of the effectiveness of internal controls. These place major responsibility on the CFO, the company's main compliance gatekeeper. And on the company's external auditors who must provide a public opinion about the reliability and effectiveness of the company's internal controls. What is internal control? These are not only policies and processes – but internal control may also include the company's IT systems and records retention technologies. A lack of good records retention or document management technology might imply a serious lack of reasonable internal controls for an auditor or an investigator.

SOX does not spell out technology requirements for records retention, but it does imply that companies are expected to exercise strong control over all the records and information that is used to produce financial reports. And again, this is not limited to financial spreadsheets in the accounting department. It extends to marketing and sales reports, internal memos, even instant messaging, and just about every type of file produced by your employees.

SOX – Section 409

Section 409 mandates significantly expanded disclosure requirements, with disclosures made as quickly and completely as possible after an event affects the company's performance. Once again, SOX is making a big assumption that companies have almost real-time visibility into their company's data, including all sorts of situations and business transactions that are outside the direct control of the accounting or finance functions.

For example, let's say that a marketing manager in your European office is made aware that 500 of your company's industrial pumps are about to be recalled due to an engineering defect. The pumps cost $100,000 each. That recall is very likely to have a material effect on the company's financial performance. As soon as the company is aware of this event, SOX requires that it be disclosed publicly, generally within a matter of a few days.

This has created a demand for more advanced business intelligence systems that actively look across your entire enterprise for events – positive or negative – that may affect your company's financial results. This, too, puts new demands on IT systems and especially the speed of data access.

SOX – Sections 103a and 801a

Sections 103 (a) and 801 (a) require public companies and registered public accounting firms to maintain audit work papers, documents that form the basis of an audit or review, and all information supporting conclusions for at least 7 years.

SOX – Section 802

Section 802 makes it a crime for anyone to intentionally destroy, alter, mutilate, conceal cover up or falsify any records documents, or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing. Section 802 underscores the importance of record retention and destruction policies that affect all of a company's Email, Email attachments, and documents retained on computers – e-data – as well as hard copies of all company records.

The rules state that if you know your company is under investigation, or even suspect that it might be, all document destruction and alteration must stop immediately. And, you must create company records showing that you've ordered a halt to all automatic e-data destruction practices. Institutions also need to consider all other regulatory rules governing records retention within their industry. For example, for FFIEC, SEC, IRS, etc…most documents must be retained for 7 years.

Record Retention Requirements and Time Periods

The federal government views just about any type of company information as a business record. This certainly includes business documents, in hard copy and electronic form, as well as many other types of electronic files you may not think of as a business record – but the government does. E-data is also subject to disclosure in lawsuits with non-government opponents in federal and state courts, just like traditional paper documents.

Primary Classification List of Records to Be Retained

There are hundreds of document types that may factor into an investigation or legal action. Such records are assumed to be searchable and quickly available upon request, under the rules of SOX. This even applies to less official types of records, like Emails or instant messages.

Some of the records types and retention time periods for physical and/or electronic records are:

Record Classification Types	Retention Period
Accounts Payable Ledger	7 years
Accounts Payable Transactions	7 years
Accounts Receivable Ledger	7 years
Accounts Receivable Transactions	7 years
Accountant Audit Reports	Permanently
Bank Statements	7 years
Capital Stock and Bond records	Permanently
Charts of Accounts	Permanently
Contracts and Leases	Permanently
Correspondence (legal)	Permanently
Deeds, Mortgages, Bills of Sale	Permanently
Employee Payroll Records	Permanently
Contractor Payment Records	7 Years
Employment Applications	3 years
Inventory Records (products)	7 years
Insurance Records	Permanently
Invoices to Customers	5 years
Invoices from Vendors	5 years
Patents	Permanently
Payroll Records and Tax Returns	7 years
Purchase Orders	5 years
Safety Records	6 years
Time Cards and Reports	7 years
Training Manuals	Permanently
Union Agreements	Permanently

Record Classification by Device and Location

The record classification system considers the types of Devices/media, location, approval for use, and limitations.

Device/Location	Approved	Limitations
Enterprise Device	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not use it for any personal or non-business-related purpose. All data that resides on enterprise devices is (and becomes) the property of the enterprise. All information is confidential and sensitive and should not be distributed outside of the enterprise without the expressed authorization of the enterprise.
Enterprise approved BYOD	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements. This also means the BYOD meets all security and mandated government and industry requirements.	Limit access to the BYOD device to only authorized and approved users. No games or installation of applications in which the device and the data could be contained on it at risk.
Enterprise e-mail	Use the enterprise email account to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not conduct any personal business on the enterprise email account. Never open an unknown attachment or reply to anyone unknown to you.
Enterprise Cloud Storage	Use enterprise cloud storage to access enterprise information	Do not store personal information on enterprise cloud storage.
Personal Cloud Storage	For personal use only	Never store enterprise information on personal cloud storage

What ENTERPRISE Should Do

First and foremost, ENTERPRISE should have a written policy devoted to data retention. The record management, retention, and destruction policy should cover the following:

- Purpose of the policy
- Who is affected by this policy
- What type of data and electronic systems are covered by this policy
- Define key terms especially legal and technical terminology
- Describe the requirements in detail from the legal, business, and personal perspective
- Outline the procedures for ensuring data is properly retained
- Outline the procedures for ensuring data is properly destroyed
- Document the litigation exception process and how to respond to discovery requests
- List the responsibilities of those involved in data retention activities
- Build a table showing the information type and its corresponding retention period
- Document the specific duties of a central/corporate data retention team if one exists
- Appendix for additional reference information

Record Classification, Management, Retention, and Disposition Standard

Both employees and management rely heavily on the records generated as a result of the business and operation of ENTERPRISE. These records document ideas and activities to help ENTERPRISE better serve its mission, meet mandated requirements, assist management in its decisions making and act as an archive of ENTERPRISE's history. Records, like any vital resource, also have an intangible monetary value. Because of the tangible and intangible value of ENTERPRISE records, they must be part of a comprehensive Record Management program that ensures all ENTERPRISE records are properly and securely managed, replaceable (in the case of vital records), disposed of, preserved, and/or archived.

ENTERPRISE Record Classification and Management program serves other purposes as well. It improves office efficiency, facilitates administrative access to inactive as well as active records, ensures the consistent maintenance of records, decreases operational costs, increases staff productivity, and assists ENTERPRISE in meeting legal and regulatory standards. Obsolete records impede access to current records; pose a possible legal liability, and waste valuable space.

Purpose

This standard is issued according to ENTERPRISE record classification, management, retention, and disposition policy and:

- Outlines ENTERPRISE's requirements for its record management and retention program including records creation, maintenance, organization, use, security, disposal, and archive.
- Defines criteria for the identification of vital records and the requirements for the maintenance, security, and handling of vital records.
- Provides for schedules of records retention and disposition.
- Outline criteria for the conversion of retained or archival records to a different medium (e.g., recordable disk files to DVD or optical disks and paper to fiche or scanned documents).

Scope

The scope of the record classification, management, retention, and disposition program is:

- Based on the laws of the state of _____, the United States, EU, and other regulatory agencies. Additionally, this standard complies with the applicable federal and state laws which govern the privacy, and confidentiality of individuals. If this standard conflicts with any applicable law, the law takes precedence and will apply. ENTERPRISE policies/guidelines or ENTERPRISE procedures may impose certain restrictions that are not specifically covered by state and federal law, or other regulations and must be followed in any case.
- Shall not be construed to be inconsistent with any contractual obligation of the ENTERPRISE.
- Apply to all records commonly and individually created and/or maintained by ENTERPRISE and its units.

- Includes all ENTERPRISE records regardless of the medium on which they reside (e.g., paper; fiche; in electronic form on tape, cartridge, disk, CD-ROM, DVD, or hard drive; scanned documents, etc.) and regardless of form (e.g., text, graphics, video, voice, drawings, etc.).
- Applies to all employees of ENTERPRISE.
- Refers to all record categories, which may or may not include various record types such as financial, legal, medical, employee, contract, etc.
- Functions in conjunction with other ENTERPRISE data and computing guidelines/standards; Data/System Administrator responsibilities; and system requirements and ENTERPRISE data and computing standards.

Responsibilities

ENTERPRISE record administrator(s) appointed by the Chief Information Officer shall:

- Ensure compliance with federal, and state law, and regulatory agencies concerning the preservation of ENTERPRISE records.
- Ensure compliance with these standards and related record retention and disposition schedules.
- Jointly determine which ENTERPRISE records are Institutional records.
- Jointly develop and ensure the implementation of an organization and filing procedure for ENTERPRISE records.
- Jointly designate an original record custodian (ORC) from specific ENTERPRISE departments for Original Records. For example, the Procurement Department might be the ORC for Purchase Orders and Requisitions.
- Work with ENTERPRISE departments to develop departmental retention and disposition schedules for internal records not addressed in ENTERPRISE schedules.
- Work with the administrative services and records archivists to ensure that records scheduled for disposition are reviewed to determine if the records have a continuing administrative or historical value. Records that have been determined as having such value shall be designated for archival retention and others will be properly disposed of.
- Work with the administrative services and records archivists to prepare and maintain a Record Management “manual” outlining procedures to:
- Ensure the security of original records;
- Protect irreplaceable or vital records from destruction;
- Validate the Disaster Recovery Business and Continuity Plan complies with this policy (see https://www.e-janco.com/DisasterPlanning.htm)
- Designate original records custodians for new records;
- Ensure that original records are organized in an efficient and accessible manner;
- Ensure that original records are reviewed before disposal to determine whether they are archival records;
- Transfer records, in whole or in part, from the custodian of the original records to the appropriate archive;
- Provide periodic inventories of ENTERPRISE records; and
- Assist ENTERPRISE departments in complying with this standard and its schedules.

ENTERPRISE and records archivist(s) appointed by the Chief Information Officer shall:

- Ensure compliance with state law concerning the preservation of ENTERPRISE records.
- Ensure compliance with these Standards and their related ENTERPRISE Record Retention and Disposition Schedules.
- Work with the administrative services and records administrators to ensure that records scheduled for disposition are reviewed to determine if the records have a continuing administrative or historical value. Records that have been determined as having such value shall be designated for archival retention and others will be properly disposed of.
- Jointly determine where ENTERPRISE and unit records archives will be located.
- Ensure that archival records are properly transferred to the appropriate archival storage facility.
- Ensure that archival records are stored in a facility with proper environmental (e.g., light, temperature, humidity, air quality, handling, etc.) and security controls so that the records are and remain accessible and readable by authorized personnel.
- Ensure that archival records are periodically copied so that their quality and readability are maintained. This is especially critical when the record is on magnetic media, film, or fiche.
- Validate the Disaster Recovery Business and Continuity Plan complies with this policy (see https://www.e-janco.com/DisasterPlanning.htm)
- Work with the administrative services and records administrators to prepare and maintain a Record Management "manual" outlining procedures to:
    - Ensure the security of original records; protect irreplaceable or vital records from destruction;
    - Designate original records custodians for new records;
    - Ensure that original records are organized in an efficient and accessible manner;
    - Ensure that original records are reviewed before disposal to determine whether they are archival records;
    - Transfer records, in whole or in part, from the Original Records Custodian to the appropriate archive; and
    - Provide periodic inventories of ENTERPRISE Records, and assist ENTERPRISE departments in complying with this standard and its schedules.
- Maintain a brief catalog, or list, of archived records and their location.

Record Management

Record Management is a joint responsibility of the record creator and users. All ENTERPRISE employees who handle ENTERPRISE records are responsible for knowing and following laws (i.e. Sarbanes-Oxley), ENTERPRISE policies, guidelines/standards, and ENTERPRISE procedures that govern these records.

All ENTERPRISE administrative records are owned by ENTERPRISE regardless of their physical location, even when in the possession of individuals.

ENTERPRISE records may not be permanently removed from ENTERPRISE or destroyed except per approved record management, retention and disposition standards, and schedules.

Record Management consists of 3 basic stages:

- Record Creation
- Record Use
- Record Disposition

Record Creation

When a record is created, the creator should consider the following:

- Is the new record original?
- What is the type of data included in the record being created?
- How should the record be handled and stored?
- Do any laws or regulations dictate a specific retention period?
- Barring any legal/regulated retention period, when will the information on the record be no longer useful?

Based on the answers to these questions, the record creator shall assign two classifications to the record:

- A data security classification based on ENTERPRISE levels of data classification, and
- A record retention designation based on legal, administrative, research, and historical requirements.

Neither the format of the record (e.g., memo, Email, voice recording, etc.) nor the medium on which it resides (e.g., paper, CD-ROM, DVD, fiche, audio, video, electronic, etc.) determines the records' data security classification. For example, Emails may be just as confidential as formal, typed letters.

When a new original record is created, the appropriate department will request the designation of an original records custodian (ORC) from the appropriate records administrator if one does not currently exist for the class (i.e., a series of similar records such as accounting records or payroll records) the new records applies to (e.g., if a new original record is part of a personnel file, the existing ORC for personnel files would apply). The record creator's department may or may not be the ORC for the created record.

The ORC is the department responsible for the maintenance of the original ENTERPRISE records of a specific class (e.g., the Controller's Office is responsible for the maintenance of original ENTERPRISE financial records). ORC's

also ensured that ENTERPRISE Record Management, retention, and disposition standards (e.g., record security, management, disposition, preservation/archive, etc.) are implemented for the records under their responsibility and that staff within the ORC department understand ENTERPRISE record management standards and best practices. Most original records under the responsibility of an ORC are stored in that ORC's location, however, the records may be stored elsewhere.

An ORC can be someone not in the direct employ of ENTERPRISE such as an outsourcing provider. They must also comply with this policy.

Data Security Classification

Records are made up of data. Record security (see https://www.e-janco.com/Security.htm), which includes access, use, storage, and disposition, is based on the classification of the data in the record. If a record contains data of multiple classifications, the record will be assigned the most secure data security classification level. ENTERPRISE records are classified as:

- **Unclassified** - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific data custodian approval.
- **Operational Use Only** - data whose loss, corruption, or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which ENTERPRISE had determined is critical to its business and requires a higher degree of handling than unclassified data. Access to Operational Use Only data is available to data custodian-approved users only.
- **Confidential** - data whose loss, corruption, or unauthorized disclosure would be a violation of federal or state laws/regulations or ENTERPRISE contracts (i.e., protected data); personally identifiable data; data that involves issues of personal privacy; or data whose loss, corruption, or unauthorized disclosure may impair the academic, research or business functions of the ENTERPRISE, or result in any business, financial, or legal loss.

Many records are created during "normal administrative practices" and are either for extremely short-term use (i.e., transient records such as calculations) or contain unimportant information. Additionally, many records are received from external sources (e.g., advertisements, vendor sales materials, etc.) that have no significance to ENTERPRISE or its records needs, and therefore retention of these materials may be unnecessary.

The majority of administrative practice records have a data security classification of Unclassified and include:

- Superseded vendor manuals or instructions.
- External reference materials include catalogs, periodicals, and trade journals.
- Information copies of press cuttings, press statements, informational bulletins, or publicity materials.
- Letters of appreciation or sympathy, or anonymous letters.
- Calendars, office diaries, and appointment books (unless identified as historically important information).
- Rough drafts of reports, draft correspondence, notes, routine or rough calculations including only data with an unclassified security classification.
- Email SPAM
- Routine Email or telephone messages not including any data other than unclassified data.
- Records were determined not to have any historical value.
- Work procedures, office assignments, and work schedules.
- Letters of transmittal (e.g., transmittal of faxes).
- Blank forms are kept for supply purposes.
- Personal or private papers neither created nor received in connection with ENTERPRISE business (e.g., birthday cards).

Records that are already in the public domain and/or available via a website or published document such as mission statements, charters, constitutions, ordinances, statutes, regulations, procedures, published directories, published reports, press releases, timetables, presentation materials, published catalogs, and data which have been redacted, also have a data classification of Unclassified.

Personal notes of a non-business nature of employees are NOT subject to most statutes and can be maintained personally, not in “original” files.

If there is any doubt about which data security classification or retention designation data falls into, contact the appropriate ORC.

Record Retention Designation

Record retention period designations are assigned according to legal, fiscal, historical, and administrative values and requirements. Record retention designation requirements are documented on Record Retention and Disposition Schedules.

The retention periods prescribed in the Record Retention and Disposition Schedules are based on years unless otherwise noted and are exact retention periods, which means that the department must keep a record for at least as long as the scheduled retention period (minimum), but no longer (maximum) unless impractical or unfeasible to do so. Variances in retention should be approved and documented by the Records Administrator as part of a Department's record retention and disposition schedule. ORCs and holders of convenience duplicate or multiple copies of expired records must appropriately dispose of these expired records within 3 months after the retention period is met. The maintenance of records beyond the retention requirements defined in ENTERPRISE record retention and disposition schedules presents a significant risk to the security and integrity of sensitive and confidential data and increases ENTERPRISE's legal liabilities.

Two types of record retention and disposition schedules are in place at ENTERPRISE:

- **ENTERPRISE Record Retention and Disposition Schedules** – schedules that pertain to commonly used ENTERPRISE-wide records (e.g., accounting, personnel, contract records, etc.). The schedule applies to all ENTERPRISE maintained records regardless of the department at which they are created and/or maintained, and applies to original and retained convenience copies, duplicate and multiple copies of records. The majority of administrative practice records may not be included in the records retention schedule because they are not stored for long-term use and have been assigned a record retention designation of Transient or Temporary.
- **Departmental Record Retention and Disposition Schedules** – schedules that pertain to records created and used within a single department and not already included in the ENTERPRISE record retention and disposition schedule.

No records list can be exhaustive and all-inclusive. Questions regarding the retention period for any specific record or class of records not included in these schedules should be addressed to the appropriate Records Administrator or ENTERPRISE legal counsel.

Record retention designations assigned to records and used in both ENTERPRISE record retention and disposition schedules and departmental record retention and disposition schedules are:

- **Permanent** - records that will be kept indefinitely. This designation is given to all records that the Central Administrative Services or Records Administrator and Archivist have determined as having continued historical or administrative value. Most records with a permanent retention period that are not actively being used/referred to should be transferred to ENTERPRISE or the unit records archive. Records with a permanent retention period that continue to be used or periodically referred to may, however, be maintained in the offices of the ORC. Note that regardless of where the Permanent record is stored, the record must be accessible regardless of medium (e.g., paper, electronic, microfilm, fiche, etc.) or type (e.g., audio, video, text, graphic, etc.). This means that not only do the records have to be available but the means to read the records (i.e., the program to access an electronic record must be able to run on current technology) must be available. The Disaster Recovery Business and Continuity Plan must include provisions for these records.
- **Until Superseded** - records that are routinely updated or revised and where the previous version has no continuing value.
- **Specific** - records that will be kept for a specified number of years. The Retention and Disposition Schedule notes the specified number of years.
- **Temporary** - records that need to be retained for a short period and that do not fall into the other record retention designations. These records should be disposed of after 6 months from the last date of entry on the record. These records have such a short retention period that they may not be included in ENTERPRISE/Department Record Retention and Disposition Schedules.
- **Transient** - records that do not need to be retained because they are used to create other retained records (drafts, notes, etc.) or whose content has no importance or relevance to ENTERPRISE business or history (e.g., external advertisements, vendor sales materials, etc.). These records are of such an extremely short-term or irrelevant nature that they are not included in ENTERPRISE/Department Record Retention and Disposition Schedules and should be immediately disposed of.

ENTERPRISE employees are required to comply with and reference ENTERPRISE and department record retention and disposition schedules to determine the length of time a particular class of records must be maintained and the final disposition of a record.

Convenience records, multiple copies, or duplicate copies do not have to be retained, however, if they are retained their management/handling must comply with ENTERPRISE Record Management standards, and they cannot be retained longer than the retention period detailed in the ENTERPRISE record retention and disposition schedules.

Notwithstanding a maximum retention period, records related to or involved in litigation, criminal or civil investigation, audit, or need for ongoing administrative purposes shall be retained. There is NO exception to the requirements for the minimum retention of a record.

Individuals involved in the retention and disposition of original records of ENTERPRISE should be aware that it is a crime to knowingly destroy, alter, or cover up a record with the intent to impede, obstruct, or influence an investigation or the administration of any matter.

The record retention periods may change as ENTERPRISE or departmental functions change and become more diverse, as laws change, and as new classes of records are created.

Vital Records

A record is vital when it contains information needed to: establish or maintain continuity of operation in an ENTERPRISE office, department, or function; recreate ENTERPRISE's legal and fiscal records; or preserve the rights of ENTERPRISE, its Board, management, and/or staff. The inability to recreate an authentic replacement of a lost or unavailable vital record could so adversely impact ENTERPRISE that extraordinary precautions are required to preserve and protect these records from both normal and unusual hazards, present and potential. The number of truly vital records should be very small concerning the total records held in any department. It should be noted that vital records follow the same retention and disposition schedules used for all record types. The fact that a record is considered vital does not necessarily mean that its retention is permanent. Data custodians, in conjunction with the appropriate Records Administrator, identify records as vital.

There are two types of ENTERPRISE vital records:

- **Records are essential to the protection of the rights of individuals**. These include, but are not limited to: current payroll records necessary to pay employees; and employee service records required for retirement status.
- **Records that are essential to the protection of ENTERPRISE's rights, assets, and/or the execution of its contractual obligations**. These include, but are not limited to: drawings and specifications required to repair and maintain ENTERPRISE's facilities; records necessary to establish ENTERPRISE's ownership of buildings, equipment, and land; patent license agreements; and promissory notes and evidence of other receivables.

Pre-identified vital records

Departments maintaining original records considered to be vital records shall ensure they are protected per these Standards. This list of pre-identified vital records is not intended to be all-encompassing. For questions regarding vital records contact the Records Administrator.

Methods of Protection of Vital Records

When determining the best way to protect vital records, Records Administrators and ORCs should consider the:

- The effectiveness of the protection method to the cost of that protection.
- Need for accessibility - Vital records that need to be available for use at all times may require different methods of protection from infrequently used vital records.
- Length of retention - Vital record retention may be short-term, long-term, or permanent and the most appropriate method of protection may differ based on the assigned retention period.
- Record Medium - The susceptibility of records to destruction from heat, water, chemicals, and aging varies depending on what medium the record was created on. Magnetic tape, CD-ROM, DVD, microfilm, and paper documents require different protection to ensure they are usable.

Six methods of records protection may be used to preserve vital records. Multiple methods can be used to protect the same types of vital records (i.e., the active financial records can be protected via the existence of duplicates while the inactive portion through the preservation of computer data that can be used to reconstruct a document). If it is not feasible to implement methods 1, 2, 3, or 4, methods 5 or 6 should be used to provide at least a minimum level of protection.

1. **Preservation of existing duplicate copies at another location**. Many records already have a form of "natural protection" because of the regular paperwork routine (e.g., equipment records at the facility administrator's office and ordering departments). If such duplicates exist for a vital record class the preservation of those duplicates is very effective protection. The likelihood of both copies being destroyed at any one time is extremely low. This method is equally effective for long- and short-term retention, durable or fragile records, and high- or low-access requirements.
2. **Creation of special duplicate copies for preservation at another location**. Special, duplicate "security" copies of many ENTERPRISE records classes may be created via photocopying, microfiche, magnetic tape backups, scanning, etc. This kind of protection is as effective as method 1 however; the cost of creating duplicate copies is relatively high.
3. **Preservation of source records which would be used to reconstruct vital records**. In many cases, information that is the source for vital records (e.g., data stored in the Human Resources system) is held by ENTERPRISE or by another enterprise (e.g., outsourcing service provider). If such sources can be identified and agreements made on holding them for the length of time protection is required, this method of protection can be nearly as effective as maintaining actual document copies. Effectiveness is reduced only slightly because several sources may be involved, any one of which might be destroyed. The overall cost of this method may be higher than the use of "natural protection" copies because larger volumes of source records may need to be retained for longer periods than may ordinarily be the case. The cost of this method, however, will usually be much less than the cost of creating special duplicate security copies.

4. **Storage in special equipment such as fire-resistant cabinets, safes, or vaults**. Original and unique copies of vital records can be protected from most hazards through the use of special storage equipment. While the protection is not absolute, its relative effectiveness is only slightly lower than the first three methods. The use of special storage equipment is usually the most costly of all preservation methods and should only be considered when the other 3 methods above are not feasible.
5. **Removal of hazardous conditions from the storage area**. By removing unnecessary hazards such as combustible materials and steam or water pipes and by eliminating undesirable conditions such as airborne chemicals and extremes of heat or humidity, a relative improvement can be achieved in the protection of records. Since the effectiveness of this method is low, it should be considered only when other methods are not feasible.
6. **Relocation of records to a less hazardous area**. Because of differences in construction and use, some ENTERPRISE buildings are less hazardous for record storage than others. The effectiveness of relocation can be equal to or slightly better than that of the removal of hazardous conditions. The cost will be equally low. However, when requirements exist for frequent access to the records, this method may prove unfeasible. If relocation is considered, the Record Administrator should be consulted to determine the environmental controls and security of various storage options.

Record Use

Records organization is one of the most important components of Record Management having a major effect on information use, accessibility, staff productivity, and the effective management of records from creation to disposition. Records Storage and retrieval involve the arrangement of information/records, the process that leads to storing information/records, the equipment/facilities in which the records are stored and the process used to retrieve the records.

Records Administrators and Archivists will work with ENTERPRISE departments to develop records storage and retrieval procedures which result in the:

- Efficient, economical, secure, and accessible records organization.
- The department's ability to effectively and properly maintain and dispose of records on an ongoing basis.

These procedures should include but are not limited to determining: what records should be retained and stored; how records should be organized in storage so that they are properly secure and accessible; how inactive records (i.e., records within their retention period but that are not used within one year) are stored; how "expired" records (i.e., records meeting their retention period and ready for disposition) leave the file and get reviewed by the Records Administrator and Archivist for proper disposition; and how non-archived expired records are appropriately disposed of (i.e., recycle, destroy).

The ORC, in conjunction with the record administrator and ENTERPRISE legal counsel, may determine that specific records (e.g., those with a 7-year or Permanent retention period, or those related to a legal investigation or audit) should be converted to another medium (e.g., microfiche, scanned document). In determining whether an archived record should be converted to another medium the following criteria should be considered:

- The legality of converting original records to another medium.
- The original medium of record and its vulnerability to compromise.
- Historical nature of the record.
- Length of record retention (i.e., the conversion is favored for long-term or permanent retention records).
- Need for accessibility.
- Available space for record storage (conversion to another medium may save space).

Original Records copied to a more permanent medium (e.g., from paper to optical disk, etc.) shall be transferred to the appropriate records archivist so that the original records can be properly destroyed.

Record Disposition

Disposal of "expired" records must be performed on a timely basis as failure to do so can lead to the unnecessary expenditure of resources (e.g., space, staff time) and liability (e.g., requests for information for legal proceedings). As previously noted, all original, convenient, duplicate and multiple copies of expired records shall be properly disposed of within 3 months of the record retention period being met.

When an original record(s) has/have met its/their designated retention period in the appropriate ENTERPRISE record retention and disposition schedule, the ORC shall review the record(s) to determine if it/they have an archival "status" (i.e., have continuing administrative, research or historical value, or document ENTERPRISE's organization, functions, policies, decisions, procedures, or operations). ENTERPRISE records retention and disposition schedules refer to retention periods for original and retained convenience records; however, the review of records for determination of archival "status" will be performed on original records only. Convenience records that have reached their designated retention period will be appropriately destroyed.

ORCs must obtain approval for the transfer/destruction of records for which they are responsible to the appropriate Records Administrator and Archivist.

Non-Archival Records

After review by the appropriate Records Administrator and Archivist or their designee, original records that are determined to be non-archival records shall be properly disposed of (e.g., recycled, destroyed) per the classification of the data contained on the record.

Archival Records

Depending on the disposition noted in the corresponding record retention and disposition schedule, acceptance of original records at disposition time by a unit or ENTERPRISE Archivist may be either optional or required. If the record retention and disposition schedule notes that the document is archival, it will automatically be transferred to an archive. If the schedule notes a retention period of permanent, the record(s) may be transferred to the archive after 7 years.

All other original records shall be reviewed by the appropriate Records Administrator and Archivist, or their designee. Original records that are determined to be archival records shall be transferred to the appropriate archive. The Records Administrator and Archivist will coordinate the transfer of archival records from the ORC to the appropriate archive. Records transferred to archives continue to be the property of ENTERPRISE.

Access to and security of records in the archive continues to be based on the data security classification of the record. Access to Operational Only and Confidential records requires ORC approval.

Records in the archive must be accessible regardless of medium (e.g., paper, electronic, CD-ROM, DVD, Optical Disk, microfilm, fiche, etc.) or type (e.g., audio, video, text, graphic, etc.). This means that not only do the records have to be available but the means to read the records (i.e., the program to access an electronic record must be able to run on current technology) must be available. Record conversion to another medium may be desired for archived records. As previously noted, the ORC, in conjunction with the unit record administrator and ENTERPRISE legal counsel, determine whether specific records should be converted to another medium based on the criteria noted above.

Records in the archive should be copied periodically to ensure that their quality and readability are maintained. This is especially critical when the record is on magnetic media, film, or fiche.

Record Destruction

All non-archival original, convenience, duplicate, or multiple copies of records that are scheduled to be destroyed must be destroyed per the record's data security classification. Unclassified and Operational Use Only records may be recycled. Confidential records must be destroyed by the following methods depending on the medium (e.g., paper, microfiche, disk, etc.) on which they were created:

- cross-shredding,
- chemically destroying or incinerating in an environmentally safe method,
- Degaussing, pulverizing, cutting, or wiping electronic files or media (e.g., tapes, CD-ROM, DVD, Optical Disks, hard drives, etc.)

When contracting with an external entity for record destruction, the contract should specify destruction measures consistent with these standards and should provide for some form of compliance monitoring and verification of record destruction.

Compliance and Enforcement

No organization operating in the United States, regardless of size or industry, is immune from the obligation to retain electronic content per the Federal Rules of Civil Procedure (FRCP). The FRCP is a body of rules and procedures that govern civil lawsuits in United States district courts.

The FRCP creates obligations on the part of all organizations to locate, preserve, and produce, promptly, electronic information relevant to the subject matter of a lawsuit.

Compliance and enforcement information is a best practice that is managed by the Chief Information Officer with support from the Internal Audit Department. Also, this policy and supporting procedures are reviewed at least annually by the legal counsel of ENTERPRISE.

Legal Definitions

- **A litigation hold** is a process used by organizations to advise their employees of anticipated litigation and ensure that relevant records are not destroyed.
- **Legal discovery** is part of the pretrial phase in a lawsuit. During legal discovery, the parties can request documents and other evidence from the opposing side. They can also compel the production of evidence by using discovery devices such as requests for production and depositions of witnesses.
- **Spoliation** is the accidental or intentional destruction or significant alteration of evidence or the failure to preserve property for use as evidence in pending or foreseeable litigation.

  If a party cannot present relevant evidence at trial because the opposing party failed to preserve it or destroyed it, an adverse inference instruction from the court permits a jury to infer that such evidence would have been harmful to the opposing party.

Email Retention Compliance

ENTERPRISE Email that is created in connection with the transaction of ENTERPRISE business is considered the property of ENTERPRISE. Records are to be maintained and disposed of according to ENTERPRISE-approved records retention and disposition schedules.

For legal reasons, it is paramount for ENTERPRISE to meet legal requirements and thus retain email and business records for a period that meets any mandated periods. Standards and procedures include the following:

- Designate individual e-mails and records as legal records.
- Capture and store all legal records in an archive (electronic or paper) for a period that exceeds legal requirements plus one day.
- Encrypt data in the legal record data store.
- Maintain and audit the ongoing security of the legal record data store.
- Provide an audit trail to the legal record data store for all additions, changes, deletes, and accesses.
- Implement a legal record data store record destruction/disposal policy in concert with ENTERPRISE's legal counsel, internal auditors, external auditors, and Board of Directors.

Policy

Many Emails are created during "normal administrative practices" and are either for extremely short-term use (i.e., transient records such as calculations) or contain unimportant information. Additionally, many Emails are received from external sources (e.g., advertisements, vendor sales materials, etc.) that have no significance to ENTERPRISE or its records needs, and therefore retention of these materials may be unnecessary.

All other Emails, and business records, fall within the Business Record Retention and Destruction Guidelines.

Since electronic storage space is limited within ENTERPRISE, all email that is not considered a business record MUST BE DELETED if it is over 59 days old. Copies of email are NOT to be saved in an electronic format by an employee within the enterprise beyond that period without a handwritten (not electronic) authorization of the enterprise's legal office and an officer of the enterprise who binds the enterprise.

The ENTERPRISE reserves the right to monitor all electronic mail retention and take appropriate management action, if necessary, including disciplinary action for violations of this policy up to and including termination.

Unclassified – Temporary

Many administrative practice records have a data security classification of Unclassified and include:

- Superseded vendor manuals or instructions.
- External reference materials include catalogs, periodicals, and trade journals.
- Information copies of press cuttings, press statements, informational bulletins, or publicity materials.
- Letters of appreciation or sympathy, or anonymous letters.
- Calendars, office diaries, and appointment books (unless identified as historically important information).
- Rough drafts of reports, draft correspondence, notes, routine or rough calculations including only data with an unclassified security classification.
- Email SPAM
- Routine Email or telephone messages not including any data other than unclassified data.
- Records were determined not to have any historical value.
- Work procedures, office assignments, and work schedules.
- Letters of transmittal (e.g., transmittal of faxes).
- Blank forms are kept for supply purposes.
- Personal or private papers neither created nor received in connection with ENTERPRISE business (e.g., birthday cards).

Email to Be Deleted

- Junk mail (SPAM)
- Personal messages
- Unclassified
- Duplicate copies
- Confirmation of appointments
- Records with short-term value, when reference value has ended. For a definition of a record with short-term value.
- Records that are past their scheduled retention time

Email to be maintained

The purpose of retaining records has to do with the value of a record. There are administrative, fiscal, legal, and historical reasons for maintaining records for time periods.

If the information contained in the Email-only exists in Email form the creating party is responsible for maintaining the record according to approved retention schedules. Unless comments are added, the copy would be considered a reference copy, and the original considered the record.

Before deleting or destroying any document (Email), ask these three questions:

1. Could this document help make it clear how a business decision was made?
2. Could this document help me support or justify my actions?
3. Could this document form part of a financial, legal, or business audit trail, claim, or obligation?

This would include documents that issue policy, ENTERPRISE decisions, outline procedures, show action, or give guidance.

A YES or MAYBE to any of the three questions above indicates that the document most likely is to be retained and disposed of according to either a departmental program schedule or the record retention schedule.

Email to be printed

- Any document with a retention schedule of three years or more
- Any document that is scheduled to go to the Archives

Regulations and Industry Impact

Regulation	Industry Impacted	Retention Implications	Penalties
Sarbanes-Oxley	All publically-traded companies	Audit records must be maintained for 7 years AFTER the audit	Fines up to $5,000,000 & imprisonment up to 20 years
Section 17a-4	Financial Services	Email records must be kept for 3 years, trading records thru the end of the account plus 6 years	Case by case
HIPAA	Healthcare	Hospital records must be kept for 5 years, medical records for the life of the patient plus 2 years	Fines up to $250,000 & imprisonment up to 10 years
Affordable Care Act	Healthcare Providers & Employers	Medical records for the life of individual plus 2 years or 30 years whichever is greater	Open to rules as they are set
FERPA	Education	Protects the privacy of student education records.	Can hold the Institution or individuals liable under other statutes or common law tort
Gramm-Leach-Bliley (GLB)	Financial Services	The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter	Fines up to $100,000 for each violation, officers, and directors can be fined up to $10,000 for each violation, and imprisonment for up to 5 years, a fine, or both

Regulations and Industry Impact Table

Keys to Email Archiving Compliance

Four objectives must be met. They are:

- **Discovery** - Information must be easy to access and consistently available to meet legal discovery challenges from regulatory committees.
- **Legibility** - Information must have the ability to be read today and in the future, regardless of technology. When selecting archiving technology, companies should look for solutions that are based on open systems, if their Email application should change. For example, if a company migrates from Microsoft Exchange to Lotus Notes, it must still be able to quickly access and read archived Emails.
- **Auditability** - An Email archiving solution must have the ability to allow third parties to review the information and validate that it is authentic.
- **Authenticity** - Information must meet all security requirements, account for alteration, and provide an audit trail from origin to disposition. An audit trail can track any changes made to an Email.

Implementation Interview Checklist

To completely understand the scope of the Record Management process interviews need to be conducted with all individual roles and departments within the enterprise. A checklist of the questions to be asked in the interviews includes:

Interviewee Questions

- ✓ Name
- ✓ Role in enterprise
- ✓ Length of time in that role
- ✓ Scope of the current role
  - Size of function
  - Departments and others the individual interacts with
- ✓ Description of responsibilities
- ✓ Previous positions in the enterprise and the length of time in those positions – brief description

Records Accessed

- ✓ What systems/applications are utilized in this function?
- ✓ What records are accessed?
- ✓ Who "owns" the records? Who can add, change, or delete records
- ✓ Size of the records "universe"?
- ✓ What security is in place for access to records?
- ✓ Can records be copied or removed? Controls?
- ✓ What other functions within the enterprise have access to those records?

Records Created

- ✓ What records are created?
- ✓ Quantity per day? Week? Cumulative?
- ✓ What systems/applications are utilized in the creation?
- ✓ How are the records stored? Electronically? Paper?
- ✓ How long and where are the records stored?
- ✓ What functions within the enterprise depend on those records?
- ✓ Who can add, change, or delete the records?
- ✓ Is there an audit trail on the recorded history for add, change, and delete?
- ✓ Security for access to records?
- ✓ The review process for accuracy?

Record classification, management, retention, and disposition Annual Review Process

Understand all the requirements for every type of record your organization has

An enterprise is faced with many mandated Record Management requirements from all levels of government, industry requirements, and best practices. Not only do governmental agencies have the ability to audit, but also judges in legal proceedings can require an audit. Know the extent of those audits and the output the company will be required to produce. Enterprises need to have the ability to work their way back through all their policies and practices to validate they can comply with all the requirements of the audits.

Develop and maintain clear and well-documented Record Management policies

The policies should include:

- Retention and disposition lengths and policies
- Records access and security policies
- Testing criteria for compliance with policies and practices
- Training requirements: For example, training criteria; for employees with access to records that have HIPAA Record Management information

Get management concurrence on those policies.

This concurrence must be based on management's understanding and agreement that:

- Record Management is a core requirement of the business, like human resources, sales, or any other key function.
- The enterprise has the organizational and legal requirements to take direct responsibility for meeting all records reporting and compliance requirements.
- The enterprise's management understands, at the highest levels, the costs and penalties for being unable to comply with Record classification, management, retention, and disposition.

Annually review your Record Management practices

Annual reviews of Record classification, management, retention, and disposition should ensure the enterprise has the policies and procedures, systems and technologies, and facilities in place to meet all operational, legal, and regulatory obligations.

This review should answer questions, such as:

- Are records complete?
- Are records use managed in compliance with Record classification, management, retention, and disposition policies
- Did the review identify security breaches in your Record Management policies?

Review systems, technologies, and facilities, as well as your practices.

The key question to ask here is, "Do your Record Management systems and technologies support your basic internal and external compliance requirements?" For example:

- Do they provide ways to track and audit retention management?
- Do they automate and enforce records destruction policies?
- Do they enforce security requirements, such as access control and tracking with recording and audit for physical and electronic records, and security for modification and deletion rights with tracking?

Document the results

Provide documentation that shows retention, disposition, security, and other record management practices, and disposition are compliant with the policy. It also, shows how the enterprise validated that the policy that is in place is correct.

Document the review process itself, including roles and responsibilities, as part of your larger Record Management practices documentation. In large organizations with internal audit groups and smaller companies that lack such groups, documentation clarifies who is responsible for conducting reviews and audits, what types of documents and records they are required to produce, and the formats in which they should be produced and reported.

Record Management Best Practices

A best practice typically meets three key criteria: it is sensible and logical, low-risk, and in widespread use. Although policies vary based on business circumstances; the best practices that we have defined are:

Engage key managers and record stakeholders

Successful record management, retention, and destruction system must incorporate input from a variety of stakeholders both inside and outside the IT department. Understanding the intent of the solution is necessary for a successful outcome, whether it is for litigation readiness, regulatory compliance, business productivity, or perhaps all three. A variety of inputs will likely broaden the scope of the solution, increasing its impact on the business. Create a steering committee from the outset consisting of both in-house and outside legal counsel, human resources, finance, compliance, and Record Management officers, and key individuals from all lines of business as well as the information technology staff.

Especially important is the creation of a bridge between legal and information technology. Since record management, retention, and destruction solution could serve as a litigation e-discovery repository as well as for the enforcement of regulatory compliance, the needs of the legal staff must be understood and met.

Define scope, needs, and Objectives

Take time to interview representatives from a wide variety of business departments. Determine what record types are currently kept, what regulations must be met, and what business needs exist for historic data retention. Discuss experiences and pain points with the current Record Management and recovery strategy.

Also use this opportunity to explain the technical and operational aspects of record management, retention, and destruction solutions so users will have realistic expectations once the solution is operational.

Litigation and compliance may discourage the deletion of data, but other priorities may outweigh this risk. For example, as a record repository grows larger it requires greater human management as well as increasing amounts of storage.

Implement metrics and monitor processes

Implement metrics that regularly monitor and report processes to ensure the maximum benefit is being obtained. Check storage capacity well ahead of time, since archiving inputs cannot wait while excess capacity is procured. Regular capacity reports will also enable a greater understanding of the volume of data being imported into the archive, potentially directing future efficiency projects. Use the capacity reports to develop forecasts for system utilization as well as operational considerations. As the volume of data in the repository increases, so will the amount

of human effort required to manage it. A long-term progression of operational reports will ensure that staff can be brought in when needed.

Generate reports to show that the archive is performing as expected, and share these with the stakeholders identified previously. If any unexpected results or failures appear, share these as well since stakeholder buy-in will be needed to support remediation plans.

Define meaningful retention periods

Start with a few simple retention periods, such as one year, five years, ten years, and indefinite. Match these timeframes to record-type requirements, making sure that minimum needs are met.

Some of the records types and retention time periods for physical and/or electronic records are:

Record Types	Retention Period
Accounts payable ledger	7 years
Accounts receivable ledger	7 years
Audit reports of accountants	Permanently
Bank statements	7 years
Capital stock and bond records	Permanently
Charts of accounts	Permanently
Contracts and leases	Permanently
Correspondence (legal)	Permanently
Deeds, mortgages, bills of sale	Permanently
Employee payroll records	Permanently
Employment applications	3 years
Inventory records (products)	7 years
Insurance records	Permanently
Invoices to customers	5 years
Invoices from vendors	5 years
Patents	Permanently
Payroll records and tax returns	7 years
Purchase orders	5 years
Safety records	6 years
Time cards and daily reports	7 years
Training manuals	Permanently
Union agreements	Permanently

See the Appendix for a fuller list of document types and retention periods.

Define search and retrieval core requirements

One of the key requirements of “world-class” record management, retention, and destruction solutions is an ability to quickly search through a wide variety of data. Searching is enabled by the use of data indexes and is enhanced with automated tagging and free-form commenting capabilities.

Consider the level to which interactive browsing, searching, or automated data tagging will be required by your users, and select an application with capabilities to match. If a proprietary interface is used for searching, weigh the amount of training that will be required to get your users up to speed.

E-discovery requires flexible and dynamic search and tagging capabilities. Legal requests for “every e-mail related to this customer” or “every file containing this keyword” are common as litigation progresses. An archiving system that tags messages or files based on criteria like customer names would be appropriate for the former request, while one that allows ad-hoc queries will be required for the latter. If e-discovery is a requirement for your archiving solution, look for one with robust capabilities in this area.

Automate the record retention and destruction processes

In today’s economic environment, employees do not have the time or expertise to manually classify and manage records. A manual process inevitably leads to an incomplete and inconsistent repository. Automated record retention ensures a uniform archiving process and increases end-user productivity. Also, most archives ensure record protection if a litigation hold is issued.

Any record management solution professing to serve the needs of regulators or litigators must contain a complete set of information. An automated archiving solution is only as good as the rules it is following, but an enterprise-wide solution is preferable to a fragmented archive. Since many record management solutions are tailored to specific applications or data types, focus on applications for which technical solutions are already available and invite widespread use.

Examples include e-mail, document management, CRM and other databases, and file servers. Some archiving solutions support multiple data types, but there is no general-purpose record repository solution for all data. Therefore, any solution will be limited by definition, but an automated solution will provide a more complete data set.

Consider also the security implications of data retention. Any data that is saved will be subject to a variety of privacy regulations, so any solution must be secure. Data security includes three primary facets: confidentiality, integrity, and availability.

Start the process with current records – add old records over time

Implementation of a record repository system need not wait for the complex and time-consuming task of creating an overall data retention policy. It is often simpler to start collecting data from all supported sources immediately rather than trying to create a perfect system and delaying implementation.

For example, if your enterprise decides to retain all e-mail for five years, it would take 5 years for the e-mail archive to fill.

Train staff

To help ensure compliance with the policy and schedule, employees, managers, and any assigned departmental records coordinators should be educated on the record retention policies and procedures. While the use of stubbing makes many archiving solutions user-friendly, employees should also be trained on the automated archiving solution. Create a training plan and develop the necessary communication tools for training various levels of employees. Policy audit processes and procedures should also be developed.

Review and update the policy at least annually

Once a policy is in place, be sure to review it annually. Regulations and laws are constantly changing, and the courts expect companies to be fully aware and prepared.

A policy should include the following standards:

- Definition of a business record
- Security and data privacy issues
- Data management and retention policies
- Staff responsibilities
- Auditing and processes for dealing with violations

Appendix

Job Descriptions

Three (3) full job descriptions are included with this policy template. They come separately in their directory.

Manager – Record Administrator

Manager WFH Support

Record Management Coordinator

Forms

Thirteen (13) Record Classification electronic forms are included with this policy template. They come separately in their directory.

Personnel Records – sections of this form have been pre-completed for areas that are mandated by US federal laws and are consistent across all industries

Administrative Records

Computer and Information Security Records

Computer Operations and Technical Support

Data Administration

General Systems and Application Development

Facility Records

Financial Records

Mobile Device Access and Use Agreement

Safety Records

Sales Records

Network and Communication Services

User and Office Automation Support

Document Retention Periods

	Years										
	1	2	3	4	5	6	7	8	9	10	PERM
Accounting Records											
Bank statements, reconciliations & deposit slips											
Dividend checks (canceled)											
Expense reports											
Monthly/interim financial statements											
Inventory count & costing sheets											
Fixed asset acquisition invoices (after disposal)											
Accounts payable ledgers (computer runs)											
Accounts receivable ledgers (computer runs)											
Cash books & cash register tapes											
Subsidiary ledgers											
Monthly trial balances											
Checks											
Payroll (individual time report & earnings records)											
Vouchers											
Audit reports											
General ledgers & journals											
Annual financial statements											
Income tax returns & work papers											
Payroll tax returns & W-2s											
Corporate Records											
Mortgages, notes & leases (after expiration)											
Bylaws, charter & minute books											
Checks (taxes, property & fulfillment contracts)											
Contracts & agreements (after termination)											
Copyrights, trademarks & patent registrations											
Deeds & easements											
Partnership agreements or corporate documents											
Labor contracts											
Capital stock & bond records											
Patents											
Proxies											
Retirement & pension records											
Correspondence											
General											
License, traffic & purchase											
Production											
Legal											
Insurance											
Policies (after expiration)											
Accident reports											
Fire inspection reports											
Group disability records											
Safety reports											
Claims (after settlement)											

	Years										
	1	2	3	4	5	6	7	8	9	10	PERM
Personnel files (after termination)											
Employment applications (not hired)											
Payroll (time cards)											
Discrimination charges (after settlement)											
Performance reviews (after termination)											
Contracts (after expiration)											
Daily time reports											
Disability & sick benefits records											
Personnel files (after termination)											
Withholding tax statements											
Employee manuals & policies (after being replaced)											
Worker's Compensation documents											
Purchasing and Sales											
Purchase orders											
Requisitions											
Sales contracts											
Sales invoices											
Shipping & receiving											
Export declarations											
Freight bills											
Manifests											
Shipping & receiving reports											
Waybills & bills of lading											

Federal Law Record Retention

Here is an overview of the files affected by US federal regulations.

Federal Acquisition Regulation

The Federal Acquisition Regulation (FAR) requires that all negotiated procurement and sealed bid contracts contain clauses requiring contractors and subcontractors (herein referred to generally as "contractors") to retain all records related to pricing, proposals, negotiations, and performance of the contract and subcontracts.

"Records" include "books, documents, accounting procedures, and practices, and other data, regardless of the type and regardless of whether such items are in written form, in the form of computer data, or any other form, and other supporting evidence to satisfy contract negotiation, administration, and audit requirements of the contracting agencies and the Comptroller General." FAR 4.703(a).

Retention Periods

The general time for retaining records is not less than three years after the final payment. For the following types of acquisition and supply records, however, the required period of retention is not less than four years:

- Work orders for maintenance and other services;
- Equipment records, consisting of equipment usage and status reports, and equipment repair orders;
- Expendable property records, reflecting accountability for the receipt and use of the material in the performance of a contract;
- Receiving and inspection report records, consisting of reports reflecting receipt and inspection of supplies, equipment, and materials;
- Purchase order files for supplies, equipment, material, or services used in the performance of a contract; supporting documentation and backup files including, but not limited to, invoices, and memoranda (e.g., memoranda of negotiations showing the principal elements of subcontract price negotiations);
- Production records of quality control, reliability, and inspection.

For store requisitions for materials, supplies, equipment, and services, the retention period is two years. For construction contracts, the following must be retained for three years:

- Payroll sheets, registers, or their equivalent, of salaries and wages paid to individual employees for each payroll period;
- Change slips;
- Tax withholding statements.

Also, in the case of construction contracts, the following must be retained for two years:

- Clock cards or other time and attendance cards;
- Paid checks, receipts for wages paid in cash, or other evidence of payments for services rendered by employees.

Job Advertisements and Postings

- According to the AMERICANS WITH DISABILITIES ACT (ADA), AGE DISCRIMINATION IN EMPLOYMENT ACT (ADEA), and FAIR LABOR STANDARDS ACT (FLSA), job advertisements and internal postings should be retained for a minimum of 1 year.

Resumes and Applications

- The ADA, REHABILITATION ACT, TITLE VII of the CIVIL RIGHTS ACT, and ADEA require employers to keep all resumes and job applications on file for 1 year. Because the ADEA further stipulates a 2-year retention period for paperwork for individuals over the age of 40 (something that may be difficult to determine and is, of course, illegal to ask), consider making it a policy to hold onto all resumes and applications for that long.

Employment Action Records

- Records relating to promotions, demotions, transfers, and terminations must be retained for 1 year according to the ADA, ADEA, and TITLE VII. While training records, in general, should also be kept on file for 1 year, those related to safety and health must be retained for 3 years per the OCCUPATIONAL SAFETY AND HEALTH ACT (OSHA).

Wage and Hour Records

- The FLSA and EQUAL PAY ACT oblige you to keep basic employment and earnings records for 2 years and payroll records for 3 years.

Tax Records

- Information relating to income tax withholdings must be retained for 4 years according to the FEDERAL INSURANCE CONTRIBUTION ACT (FICA) and FEDERAL UNEMPLOYMENT TAX ACT (FUTA).

Retirement and Pension Records

- THE EMPLOYEE RETIREMENT INCOME SECURITY ACT (ERISA) mandates that employee benefit plan information, including summary plan descriptions (SPDs) and annual reports, be kept on file for 6 years.

Leave Records

- Information relating to leaves of absence under the FAMILY MEDICAL LEAVE ACT (FMLA), such as time off and medical certification, must be retained for 3 years.

I-9 Forms

- Under the IMMIGRATION REFORM AND CONTROL ACT of 1986 (IRCA), I-9 forms must be retained for 3 years after employment begins or 1 year following termination (whichever is later).

Job-Related Illness and Injury Records

- OSHA requires that information on job-related illness and injury be kept on file for 5 years. In cases of exposure to toxic substances or blood-borne pathogens, medical exam results must be retained for 30 years after the employee's termination.

Federal Legal Citations

Law	Records/Reports	Retention Requirements
Age Discrimination in Employment Act (ADEA) **Applies to employers with at least 20 employees.**	Payroll or other records, including those for temporary positions showing employees' names, addresses, dates of birth, occupations, rates of pay, and weekly compensation. Applications (including those for temporary employment), personnel records relating to promotion, demotion, transfer, selection for training, layoff, recall, or discharge; job advertisements and postings; copies of employee benefit plans, the seniority system, and merit systems.	Three years for payroll or other records showing basic employee information. One year for applications and other personnel records. Where a charge or lawsuit is filed, all relevant records must be kept until the "final disposition" of the charge or lawsuit.
Americans with Disabilities Act (ADA) **Applies to employers with at least 15 employees.**	Applications and other personnel records (e.g. promotions, transfers, demotions, layoffs, terminations) request a reasonable accommodation.	One year from making the record or taking the personnel action. Where a charge or lawsuit is filed, all relevant records must be kept until "final disposition."
Civil Rights Act of 1964, Title VII **Applies to employers with at least 15 employees.**	Applications and other personnel records (e.g. promotions, transfers, demotions, layoffs, terminations), including records for temporary or seasonal positions. Requires the filing of an annual EEO-1 Report (for Federal contractors with 50 or more employees, and non-contract employers with 100 or more).	One year from making the record or taking the personnel action. Where a charge or lawsuit is filed, all relevant records must be kept until "final disposition." A copy of the current EEO-1 Report must be retained.
Consolidated Omnibus Budget Reconciliation Act (COBRA)	Provide written notice to employees and the dependents of their option to continue group health plan coverage following certain "qualifying events," such as the employee's termination, layoff or reduction in working hours, entitlement to Medicare, and the death or divorce of the employee (that would cause dependents to lose coverage under the employer's plan).	
Davis Bacon Act **Service Contract Act** **Walsh-Healy Public Contracts Act** **Applies to federal contractors.**	Records containing the following information for each employee: • Basic employee data to include name, address, social security number, gender, date of birth, occupation, and job classification. • Walsh-Healy requires the retention of current work permits for minors and requires the retention of data for job-related injuries and illnesses, specifically, logs with dates and summaries, and details of accidents Compensation records to include: • Amounts & dates of actual payment. • Period of service covered. • Daily and weekly hours. • Straight time and overtime hours/pay. • Fringe benefits paid. • Deductions and additions.	Three years from the end of the contract.

Law	Records/Reports	Retention Requirements
Employee Retirement Income Security Act (ERISA)	Maintain, and disclose to participants and beneficiaries and report to the Department of Labor, IRS, and the Pension Benefit Guaranty Corporation (PBGC) certain reports, documents, information, and materials. Except for specific exemptions, ERISA's reporting and disclosure requirements apply to all pension and welfare plans, including: • Summary plan description (updated with changes and modifications). • Annual reports. • Notice or reportable events (such as plan amendments that may decrease benefits, a substantial decrease in the number of plan participants, etc.). • Plan termination.	Employers must maintain ERISA-related records used to develop all required plan descriptions or reports, as well as other materials needed to certify information for a minimum of six years. Records used to determine benefits that are or will become due for each employee participating in the plan must be retained as long as they are relevant.
Employee Polygraph Protection Act	Polygraph test results and the reasons for administering.	Three years.
Equal Pay Act	Payroll records include time cards, wage rates, additions to and deductions from wages paid, and records explaining sexually-based wage differentials.	Three years.
Executive Order 11246 **Applies to federal contractors.**	Requires the preparation of an Affirmative Action Plan (AAP) for Minorities and Women. Applications and other personnel records that support employment decisions (e.g. hires, promotions, and terminations) are considered "support data" and must be maintained for the AAP.	AAPs must be updated annually; AAPs and documentation of good faith efforts must be retained for two years. Personnel or employment records must be retained for two years. If there are fewer than 150 employees or a contract is less than $150,000, the retention period is one year.
Lilly Ledbetter Fair Pay Act	Law allows employees to file charges of pay discrimination without the 180/300-day time limit.	The new law will require employers to ensure that their pay practices do not discriminate. Keeping accurate records of pay and pay increases is a critical component of the Act.
Fair and Accurate Credit Transactions Act (FACTA)	Consumer credit reports.	Recently written rules for the Fair and Accurate Credit Transactions Act (FACTA) will require every employer that employs one or more employees to shred any documents that contain information derived from a credit report. The penalties for failure to observe the shredding rules include: civil liability in which an employee can recover actual damages from his/her employer for all damages incurred from identity theft; statutory damages of up to $1,000 per employee; an employer may open itself to class action liability if a large number of employees are affected; federal fines of up to $2,500 for each violation; and state fines of up to $1,000 per employee.

Law	Records/Reports	Retention Requirements
Fair Labor Standards Act (FLSA)	Payroll or other records containing the following information for each employee: • Employee's name, home address, date of birth (if under 19 years of age), gender, and occupation • Time of day/day of the week for the beginning of the workweek • Regular hourly rate of pay or another basis of payment (hourly, daily, weekly, piece rate, commission on sales, etc.) • Daily hours worked and total hours for each workweek • Total daily or weekly straight-time earnings (exclusive of overtime premiums) • Total additions to and deductions from wages for each pay period • Total wages per paid period • Date of each payment of wages and the period covered by the payment For the executive, administrative, and professional employees, or those employed in outside sales, employers must maintain records that reflect the basis on which wages are paid in sufficient detail to permit calculations of the employee's total remuneration, and perquisites, including fringe benefits.	For at least three years.
Family & Medical Leave Act (FMLA)	Records containing the following information: • Basic employee data to include name, address, occupation, rate of pay, terms of compensation, daily and weekly hours worked per pay period, additions to/deductions from wages, and total compensation. • Dates of leave taken by eligible employees. Leave must be designated as FMLA leave. • For intermittent leave taken, the hours of leave. • Copies of employee notices and documents describing employee benefits or policies and practices regarding paid and unpaid leave. • Records of premium payments of employee benefits. • Records of any dispute regarding the designation of leave.	Three years.

Law	Records/Reports	Retention Requirements
Federal Insurance Contribution Act **Federal Unemployment Tax Act** **Federal Income Tax Withholding**	Records containing the following information for each employee: • Basic employee data to include name, address, social security number, gender, date of birth, occupation, and job classification. Compensation records to include: • Amounts & dates of actual payment. • Period of service covered. • Daily and weekly hours. • Straight time and overtime hours/pay. • Annuity and pension payments. • Fringe benefits paid. • Tips. • Deductions and additions. Tax records to include: • Amounts of wages are subject to withholding. • Agreements with the employee to withhold additional tax. • Actual taxes withheld and dates withheld. • Reason for any difference between total tax payments and actual tax payments. • Withholding forms (W-4, W4-E).	Four years from the date tax is due or tax is paid.
Immigration Reform & Control Act (IRCA)	INS Form 1-9 (Employee Eligibility Verification Form) is signed by each newly-hired employee and the employer.	Three years after the date of hire or one year after the date of termination, or whichever is later.
Occupational Safety & Health Act (OSHA) **Applies to employers with at least 10 employees.**	A log of occupational injuries and illnesses. A supplementary record of injuries and illnesses. Post a completed annual summary of injuries and illnesses. Maintain medical records and records of exposure to toxic substances for each employee.	Five years. Employee's job tenure plus thirty years.
Rehabilitation Act of 1973 **Applies to federal contractors.**	Personnel/employment records (e.g., requests for reasonable accommodation, results of physical exams, job advertisements and postings, applications, resumes, tests, test results, interview notes, and records regarding hiring, assignment, promotion, demotion, transfer, layoff, termination, rates of pay or terms of compensation and selection for training or apprenticeship). Data on complaints of disability discrimination and actions taken. Requires an Affirmative Action Plan for individuals with disabilities.	Two years. (Note: If a contractor has fewer than 150 employees or a contract of less than $150,000, the retention period is only one year.) Where a charge or lawsuit is filed, all relevant records must be kept until "final disposition." AAPs must be updated annually; no current requirement to retain expired plans.

Law	Records/Reports	Retention Requirements
Uniform Guidelines on Employee Selection Procedures	For employers with 100 or more employees, records showing the impact of the selection process for each job, maintained by sex for each racial or ethnic group that constitutes at least 2 percent of the labor force in the relevant labor area or 2 percent of the applicable workforce. For employers with less than 100 employees, records show for each year the number of persons hired, promoted, terminated, and applicants hired for each job by sex and where appropriate by race and national origin. Records include applications, tests, and other types of selection procedures used as a basis for employment decisions, such as hiring, promotion, transfer, demotion, training, and termination. Adverse impact analysis of the selection process must be conducted annually.	Where the adverse impact is found in the selection process, records must be maintained for two years after the adverse impact is eliminated. For federal contractors, during a compliance review from the Department of Labor's Office of Federal Contract Compliance Programs, data from the prior year's analysis must be available, and for the current year if a contractor is six months into its AAP plan year.
Vietnam Era Veterans' Readjustment Assistance Act. **Applies to federal contractors.**	Personnel/employment records (see Rehabilitation Act of 1973 above). Affirmative Action Plan for covered veterans. Requires the filing of the annual VETS-100 report. Job openings for positions must be listed with the state employment service.	Two years. (Note: If a contractor has fewer than 150 employees or a contract of less than $150,000, the retention period is only one year.) AAPs must be updated annually; no current requirement to retain expired plans. A copy of the current VETS-100 report must be retained.

Pennsylvania Record Retention

Pennsylvania Record Retention (35 Pa.B. 5335) From PENNSYLVANIA BULLETIN Volume 35 Number 39 Pages 5227-5366

Record retention is a matter in which an insurer's management must use prudent judgment, subject to applicable statutory requirements or restrictions. Questions concerning record retention may be directed to the Bureau of Financial Examinations, concerning financial examinations; or the Director of the Bureau of Enforcement, concerning market conduct examinations.

Guidelines for Retention of Records

Type of Record	Retention Period
Accounts Payable Ledgers and Schedules	5 years*
Accounts Receivable Ledgers and Schedules	5 years*
Advertisement Files (including Internet ads)	5 years*
Agent Commission Schedules	5 years*
Agent Contracts	5 years*
Agent Discrepancies	5 years*
Agent Licensing Records (including effective/termination dates)	5 years* (from termination)
Agent Terminations (including copies of notices to agents and the Insurance Department)	5 years*
Annual/Quarterly Statement Blank and Supporting Work papers	5 years*
Bank Reconciliations	5 years*
Borrowed Money Documents	5 years* (after the amount borrowed is paid off)
Capital Stock and Bond Records (ledgers, transfer registers, stubs showing issues, the record of interest coupons, opinions)	Permanently
Cash Books	5 years*
CPA Annual Audit Reports and Management Letters	Permanently
Charts of Accounts	5 years*
Checks (canceled)	5 years*
Checks (records of un-cashed drafts or checks)	7 years (or per escheat laws)
Checks (canceled for important payments, such as taxes, purchases of property, and special contracts)	Permanently
Claims Files (loss reports, reported and paid claims files, including a complete chronological record)	5 years*
Collateral Loans (closing documents, appraisals/valuation documents, payment history, collateral documents)	5 years* (after repayment)
Conflict of Interest Statements	5 years*
Consumer Complaints (including a log of complaints and correspondence with the state insurance department) *Note:*	5 years*

Type of Record	Retention Period
Failure to maintain a complete record of all complaints received during the preceding 4 years is a violation of the Unfair Insurance Practices Act (See 40 P. S. § 1171.5(11)).	
Contracts and Leases	5 years*(after expiration)
Correspondence with Policyholders (routine)	5 years*
Correspondence (general)	5 years*
Correspondence (legal and important matters)	Permanently
Correspondence with State Insurance Departments (other than correspondence regarding complaints)	Permanently
Duplicate Deposit Slips	5 years*
Employee Personnel Records	5 years* (after termination)
Expense Analyses and Expense Allocation Schedules	5 years*
Forms (approved by a State insurance department)	2 years (after claims can no longer be reported under the form)
General and Subsidiary Ledgers and End-of-Year Trial Balances	5 years*
Holding Company Registration Statements	5 years*
Internal Audit Reports	5 years*
Internal Insurance Records (current loss reports, claims, policies for insurance coverages purchased by the company for its protection)	Permanently
Internal Reports (miscellaneous)	5 years*
Inventories of Furniture, Fixtures, and Equipment	5 years* (after disposal)
Investment Plan	5 years*
Investment Records (buy and sell invoices, ledgers, journals, broker statements, custodial/trust account statements)	5 years*
Invoices from Vendors	5 years*
Journals	5 years*
Limited Partnership Interests (partnership agreement, partnership financial statements, records of distributions, equity valuation information)	5 years* (after disposal)
Litigation Records	Permanently
Minute Books of Directors and Stockholders (or Policyholders) and Committees (including by-laws and charter)	Permanently
Mortgage Loans (closing documents, appraisals, payment history, rent rolls)	5 years* (after repayment)
Notes Receivable Ledgers and Schedules	5 years*
Other Invested Assets (all pertinent documents)	5 years* (after disposal)
Payroll Records and Summaries (including payments to pensioners and payroll deductions)	5 years*
Petty Cash Vouchers	5 years*

Type of Record	Retention Period
Policy Issue Records (including underwriter's notes/notices, original applications, declaration pages, endorsements, and selection forms)	2 years (after claims can no longer be reported under the policy)
Policy Termination Records (including documentation)	5 years*
Policyholder Dividend Records	5 years*
Premium Notices and Refunds (including proof of refund within the required time)	5 years*
Property Records (including appraisals, costs, depreciation reserves, end-of-year trial balances, depreciation schedules, titles, plans, deeds, mortgages, and agreements of sale) (after no longer having an interest in the property)	5 years*
Rate filings (including all rates utilized during the retention period)	5 years* (after replacement by latest filing)
Reinsurance Contracts (including records of settlements, trust accounts, and letters of credit)	5 years*
Reports of State Insurance Department Examinations (financial and market conduct)	5 years*
Reserve Calculation Documentation (including actuarial opinion and supporting actuarial memorandum)	10 years
SEC Filings	5 years*
Subrogation and Salvage Records	5 years*
Surrender Request	5 years*
Tax Returns and Worksheets (including revenue agents' reports and other documents relating to the determination of income tax liability)	12 years
Unclaimed Property or Escheatable Funds/Assets	10 years
Vouchers for Payments to Vendors, employees, etc. (including allowances and reimbursements of employees, officers, or other persons for travel and entertainment expenses)	5 years*

Note: ''5 years*'' refers to 5 years from the date of the last financial examination by the domiciliary regulator or until the conclusion of a subsequent financial examination, whichever time is greater.

Massachusetts Record Retention

The doctrine of spoliation

Under the doctrine of "spoliation of evidence," a court may impose sanctions for the destruction of evidence in civil litigation based on the premise that a party has negligently or intentionally destroyed, lost, or even significantly altered evidence known or reasonably anticipated to be relevant for a pending or reasonably anticipated legal proceeding should be held accountable for unfair prejudice that results to the other party. See e.g., Wiedmann v. The Bradford Group, Inc., 444 Mass. 698 (2005)[Massachusetts case involving loss or destruction of both paper and electronic records]. The amendments to the federal rules, on which the Massachusetts rules are modeled, make it clear that spoliation applies not only to paper documents but specifically to electronically stored information as well.

When does the duty to preserve evidence arise?

The federal rules alone impose no duty on any person or entity to preserve records forever. Rather, the duty to preserve evidence generally arises no later than the time at which a defendant receives notice of the suit, or a plaintiff anticipates filing a claim. In some circumstances, the duty of a party to preserve evidence arises before the time the actual notice of a claim is received where "a litigant or expert knows or reasonably should know that the evidence might be relevant to a possible action." Kippenham v. Chaulk Services, Inc., 428 Mass 124, 127 (1998) citing Nally v. Volkswagen of Am., Inc., 405 Mass. 191, 197-198 (1989). "The threat of a lawsuit must be sufficiently apparent, however, that a reasonable person in the spoliator's position would realize, at the time of spoliation, the possible importance of the evidence to the resolution of the potential dispute." Nally v. Volkswagen of Am., Inc., 405 Mass. 191, 197-198 (1989). In the case of Wiedmann v. The Bradford Group, Inc., 444 Mass. 698 (2005), receipt of a letter from a former employee's attorney demanding payment of unpaid commissions constituted sufficient notice of a potential lawsuit.

How does a party establish that spoliation has occurred?

To obtain relief for spoliation of evidence by an opposing expert or party, the moving party must demonstrate 1) that there was a negligent or intentional loss or destruction of physical evidence (as opposed to some event beyond that party's control, such as a fire or flood), 2) that the party or expert was aware that there was a potential for litigation, and that the physical evidence was material to that litigation, and 3) that the loss or destruction of the evidence created prejudice to the moving party. See Nally v. Volkswagen of America, 405 Mass. 191, 197, 539 N.E.2d 1017 (1989). Where the moving party has established that missing physical evidence is material to its case or its defense, the court may apply a balancing test to determine the appropriate remedy. The court weighs the culpability of the party or expert to whom the fault is attributed (was it intentional, knowing, grossly negligent, or negligent), the materiality of the evidence, and the potential for prejudice. See Carbone v. Checker Taxi Company et al, Superior Court Civil Case # 90-7707E (Suffolk, December 30, 1994) (Garsh, J.).

What are the consequences?

The court has broad discretion in fashioning a spoliation remedy. Fed. R. Civ. P. 37. Sanctions include precluding the party from introducing certain witnesses or evidence, an instruction to the jury that it may infer that the destroyed evidence was unfavorable to the party that destroyed it, and an entry of judgment against the party (although this remedy, being the most severe, is reserved for the most egregious cases).

Application to electronically stored information

It is important to note that spoliation may consist not only of deliberate action on the part of a litigant but also inaction. For example, failure to halt the operation of a routine network operation may expose a party to penalties for spoliation. School districts should keep these principles, as well as state requirements for document retention (discussed below), in mind when they set their defaults for periodic and routine backup, archiving, and destruction of records that exist in electronic form, including email. The Rules of Civil Procedure do contain a so-called “safe harbor” provision which provides that parties will not face sanctions for good faith deletion and disposition of electronically stored information:

- Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

I-9 Retention

Employers must retain completed Forms I-9 for all employees for 3 years after the date they hire an employee or 1 year after the date employment is terminated, whichever is later. For example, if an employee retires from your company after 15 years, you will need to store or retain, his/her I-9 Form for a total of 16 years. *I-9 Forms* can be retained on paper, microfilm, microfiche, or electronically.

Retaining Form I-9

To store Forms I-9 electronically, you may use any electronic recordkeeping, attestation, and retention system that complies with DHS standards, which includes most commercially available off-the-shelf computer programs and commercial automated data processing systems.

Paper Retention of Forms I-9

Form I-9 can be signed and stored in paper format. When copying or printing the paper Form I-9, you may photocopy the two-sided form by making either a double-sided or a single-sided copy. You may retain completed paper forms onsite, or at an off-site storage facility, for the required retention period, as long as you can present the Forms I-9 within 3 days of an inspection request from DHS, OSC, or the U.S. Department of Labor (DOL) officers.

Retention of Forms I-9 Using Microfilm and Microfiche

You may store Forms I-9 on microfilm or microfiche. To do so you must follow DHS compliance standards.

Electronic Forms I-9

Form I-9 can be electronically generated and retained, provided subject to DHS standards, including guidelines for storing electronic I-9s. Remember, Forms I-9 must be stored for 3 years after the date you hire an employee, or 1 year after the date you or the employee terminates employment, whichever is later, which can result in a longer retention period.

Retaining Copies of Form I-9 Documentation

You may choose to copy or scan documents presented by an employee, which you must retain with his or her Form I-9. Even if you retain copies of documentation, you are still required to fully complete Section 2 of Form I-9. If you choose to retain copies of employee documentation, you must do so for all employees, regardless of national origin or citizenship status, or you may violate anti-discrimination laws.

Retaining Electronic Signature of Forms I-9

You may choose to fill out a paper Form I-9 and scan and upload the signed form to retain it electronically. Once you have securely stored Form I-9 in electronic format, you may destroy the original paper Form I-9. If you complete Forms I-9 electronically using an electronic signature, your system for capturing electronic signatures must follow DHS standards.

System Documentation

For each electronic generation or storage system used, you must maintain and make available upon request complete descriptions of the following per DHS regulations: the storage system, the indexing system, and the processes that allow for audit trails.

Security

If you retain Forms I-9 electronically, you must implement a DHS-compliant records security program.

If an employer's action or inaction results in the alteration, loss, or erasure of electronic records, and the employer knew, or reasonably should have known, that the action or inaction could have that effect, the employer has violated I-9 retention laws.

Remote Hires

It is not unusual for a U.S. employer to hire a new employee who doesn't physically come to that employer's office to complete paperwork. In such cases, employers may designate agents to carry out their I-9 responsibilities. Agents may include notaries public, accountants, attorneys, personnel officers, supervisors, etc. An employer should choose an agent cautiously since it is responsible for the actions of that agent.

Employers should not carry out I-9 responsibilities utilizing documents faxed by a new employee or through identifying numbers appearing on acceptable documents. The employer must review the original documents. Likewise, do not mail Forms I-9 to a new employee to complete Section 2 himself or herself.

Guidelines for Using Third-Party Service Providers

Some business entities contract with professional employer organizations (PEOs) to handle the personnel and benefits aspects of the business. This may include the completion and retention of Forms I-9. Where the business entity and the PEO are "co-employers," one Form I-9 should be completed between the co-employees for each employee who was simultaneously hired by the co-employees. A business entity and PEO will be deemed a "co-employer" if, among other things, an employer/employee relationship is said to exist between the business entity and PEO on the one hand, and the individual on the other, even though the employee is only performing one set of services for both co-employers. Therefore, the authority to hire or terminate employment would have to be in the hands of both the business entity and the PEO. Since both entities are employing the individual, however, both entities remain equally responsible for meeting the Form I-9 requirements and equally liable for any failures to meet those requirements.

Accordingly, the employer is fully responsible for errors, omissions, and deficiencies in the PEO's processing.

Employers should not carry out I-9 responsibilities using documents faxed by a new employee or through identifying numbers appearing on acceptable documents. The employer must review the original documents. Likewise, Forms I-9 should not be mailed to a new employee to complete Section 2 himself or herself.

Inspection

DHS, OSC, and DOL give employers 3 days' notice before inspecting retained Forms I-9. The employer must make Forms I-9 available upon request at the location where DHS, OSC, or DOL requests to see them. If you store Forms I-9 at an off-site location inform the inspecting officer of the location where you store them and make arrangements for the inspection. The inspecting officers can perform an inspection at an office of an authorized agency in the United States if previous arrangements are made. Recruiters or referrers for a fee who designate an employer to complete employment verification procedures may present photocopies or printed electronic images of Forms I-9 at an inspection.

If you refuse or delay an inspection you violate DHS retention requirements. At the time of an inspection, you must:

- Retrieve and reproduce only the Forms I-9 electronically retained in the electronic storage system and supporting documentation specifically requested by the inspecting officer. Supporting documentation includes associated audit trails that show who has accessed the system and the actions performed within or on the system during a given period.
- Provide the inspecting officer with appropriate hardware and software, personnel, and documentation necessary to locate, retrieve, read, and reproduce any electronically stored Forms I-9, any supporting documents, and their associated audit trails, reports, and other data used to maintain the authenticity, integrity, and reliability of the records.
- Provide the inspecting officer, if requested, any reasonably available or obtainable electronic summary file(s), such as spreadsheets, containing all of the information fields on all of the electronically stored Forms I-9.

Version History

2023 Edition

- Updated for WFH impact on record retention requirements
- Updated all included forms
- Updated all included job descriptions

2022 Edition

- Updated for WFH impact on record retention requirements
- Updated all included forms
- Updated all included job descriptions

2021 Edition

- Updated for WFH impact on record retention requirements
- Added job description for Manager WFH Support
- Updated all included forms
- Updated all included job descriptions

2020 Edition

- Added materials on record classification
- Updated all the electronic forms
- Updated all of the attached job descriptions

Social Networking Policy

Managing and Controlling Employee Social Networks

Janco Associates, Inc.

2023 Edition

License Conditions

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the right to use it for a SINGLE Disaster Recovery Plan unless the user has purchased a multi-user license. Anyone who makes an unlicensed copy of or uses the template or any derivative of it violates the United States and international copyright laws and is subject to fines that are treble damages as determined by the courts. A REWARD of up to 1/3 of those fines will be paid to anyone reporting such a violation upon the successful prosecution of such violators.

The purchaser agrees that any derivative of this template will contain the following words within the first five pages of that document. The words are:

Table of Contents

Policy – Social Networking

Definitions

Social Networking - Connecting with a community of people in your network through services like Facebook and Twitter with various methods of online interaction. A blog with a broad user base also is a social network

Social Media - Online media like blogs, podcasts, videos, and news with a strong participatory element through comments, ratings, or other mechanisms. Social media is generated by the people and for the people with content created by anyone with a voice.

Overview

Social networking enhances existing human behaviors for the need to connect and communicate during a crisis. Like a scene at a freeway car crash, most want to know what's happening and, in the excitement, jump in to monitor and participate.

Assume your competitors are using social networking to communicate and monitor your enterprise's social networking status. Disaster Recovery and Business Continuity Plans need to be updated to:

- Enhance Communication Plans: Just as your enterprise has an existing communication plan (often a press statement from executive management to media) understand how to repurpose these messages and communication on social networks.
- Experiment and Build a Base: Enterprises should experiment with the tools like those provided by the Department of Homeland Security and understand how to use these tools. Companies should also start to monitor, then experiment.
- Educate, Train, and build Awareness Before an Event. Companies as they test their DRPs and BCP should incorporate these social networks into the planning and execution processes. Companies need to indicate to the world what is an official channel, where people should go for news, and how each function plans to respond using these tools. These tools can help educate citizens on how to prepare for disasters, where to go for help, how to develop a crisis plan, and even basic life-saving medical techniques.

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's weblog or blog, journal or diary, personal website, social networking or affinity website, web bulletin board, or a chat

room, whether associated or affiliated with ENTERPRISE, as well as any other form of electronic communication.

The same principles and guidelines found in ENTERPRISE policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates, or otherwise adversely affects members, customers, suppliers, people who work on behalf of ENTERPRISE or [ENTERPRISE's] legitimate business interests may result in disciplinary action up to and including termination.

ENTERPRISE regards social networks as a form of communication and relationship among individuals within the company, its partners, affiliates, and customers. When the company wishes to communicate publicly as a company – whether to the marketplace or the general public – it has well-established means to do so. Only those officially designated by ENTERPRISE have the authorization to speak on behalf of the company. It is the policy of ENTERPRISE to not release confidential, sensitive, and proprietary information on social networks.

Statement

This policy applies to all employees and contractors who identify themselves or represent themselves as being associated with ENTERPRISE in

- Multi-media and social networking websites such as Twitter, MySpace, Facebook, Yahoo! Groups, and YouTube
- Social networks (Both ENTERPRISE Social networks and Social networks external to ENTERPRISE)
- Wikis such as Wikipedia and any other site where text can be posted
- All of these activities are referred to as "postings" in this Policy

Please be aware that violation of this policy may result in disciplinary action up to and including termination.

The following is the company's social media and social networking policy. The absence of or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. Consult with your manager or supervisor if you are uncertain.

- Social network postings should have clear disclaimers that the views expressed by the author in the social network are the author's alone and do not represent the views of the company. Be clear and write in the first person. Make your writing clear that you are speaking for yourself and not on behalf of the company.
- Be authentic, honest, and conversational in your posts. Leave the marketing to speak and press release format for other parts of the website.
- Use good judgment about content and be careful not to include confidential information about your company, customers, or vendors.
- Information published on social networks should comply with the company's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on blogs, forums, and other social networking sites.
- Be respectful to the company, other employees, customers, partners, and competitors.
- Social media activities should not interfere with work commitments. Refer to IT resource usage policies.
- Online presence reflects on the company. Be aware that your actions captured via images, posts, or comments can reflect that of our company.
- Do not reference or site company clients, partners, or customers without their express consent. In all cases, do not publish any information regarding a client during the engagement.

- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Company logos and trademarks may not be used without written consent.
- Listen to people and respond to as many comments as possible with constructive feedback. Allow negative comments (delete the spam) – the key to managing comments is to respond rather than censor. Avoid getting defensive and ignore the trolls where appropriate.
- Peer reviews, especially for lengthy or complicated posts, should be encouraged, but not required. It's always nice to have someone double-check grammar and technical details before it goes out to the world.

ENTERPRISE believes that everyone can both derive and provide important benefits from exchanges of perspective. ENTERPRISE personnel are personally responsible for their posts. Activities in or outside of work that affect your ENTERPRISE job performance, the performance of others, or ENTERPRISE's business interests are a proper focus for company policy.

ENTERPRISE supports dialogue among ENTERPRISE employees, contractors, partners, clients, members of the many communities in which we participate, and the general public. Such dialogue is inherent in our business model of innovation, and our commitment to the development of open standards.

- A social network is a tool individuals can use to share their insights, express their opinions and communicate within the context of a globally distributed conversation. As with all tools, it has proper and improper uses.
- While ENTERPRISE encourages all its employees to join a global conversation, it is important for those who choose to do so to understand what is recommended, expected, and required when they discuss ENTERPRISE-related topics, whether at work or on their own time. ENTERPRISE trusts – and expects – ENTERPRISE employees to exercise personal responsibility whenever they social network. This includes not violating the trust of those with whom they are engaging.
- Social networkers should not use this medium for covert marketing or public relations. When members of ENTERPRISE's Communications, Marketing, Sales or other functions engaged in advocacy for the company have the authorization to participate in social networks, they should identify themselves as such.

The Chief Information Officer or his delegate must approve all social networks and personal websites that contain references to ENTERPRISE by ENTERPRISE employees, contractors, suppliers, and or agents. This includes, but is not limited to, social networks and websites that reside on ENTERPRISE's domains or domains that are outside of the control of ENTERPRISE.

If you comment on any aspect of ENTERPRISE's business or any policy issue in which ENTERPRISE is involved and for which you have the responsibility, you must identify yourself as an

ENTERPRISE employee in your postings or social network site(s) and include a disclaimer that the views are your own and not those of ENTERPRISE. Also, ENTERPRISE employees should not circulate postings they know are written by other ENTERPRISE employees without informing the recipient that the author of the posting is an ENTERPRISE employee.

This policy applies to the entire enterprise, its employees, its agents, its vendors, its suppliers (including outsourcers), and co-location providers and facilities regardless of the ownership of the social networks and or websites.

All social networks and personal websites must follow this policy and the mandates of ENTERPRISE. Failure to comply is grounds for immediate termination, cessation of all business relationships, and the violator (and/or his organization) is subject to financial damages.

Everyone who "social networks" must complete the Social Network Policy Compliance Agreement.

Rights to content

Unless you specify otherwise, all works of authorship copyrightable by you and posted by you to any social network ("Content") are submitted under the terms of a "Public License". Under this license, you permit anyone to copy, distribute, display, and perform your Content, royalty-free, on the condition that they credit your authorship each time they do so. You also permit others to distribute derivative works of your Content, but only if they do so under the same Public license that governs your original Content.

Amongst other things, a "Public License" permits RSS aggregators to copy, distribute, display, and perform any content on the social network that you syndicate using RSS. All Content on your social network is syndicated for RSS aggregation unless you change your settings to indicate otherwise.

Confidential Information

Everyone is tasked to protect confidential information when they communicate it. Rules to follow are:

- **Make sure someone needs to know**. Do not share confidential information with other team members unless they need to know the information to do their job. If you need to share confidential information with someone outside the company, confirm there is proper authorization to do so. If you are unsure, talk to your supervisor.
- **Develop a healthy suspicion**. Don't let anyone trick you into disclosing confidential information. Be suspicious if asked to ignore identification procedures.
- **Watch what you say and discuss on social networks**. Don't have conversations regarding confidential information in public areas, forums, and blogs.

Unauthorized access to confidential information: If you believe there may have been unauthorized access to confidential information or that confidential information may have been misused, it is your responsibility to report that information.

ENTERPRISE is serious about the appropriate use, storage, and communication of confidential information. A violation of ENTERPRISE policies regarding confidential information will result in corrective action, up to and including termination. You also may be subject to legal action, including criminal prosecution. ENTERPRISE also reserves the right to take any other action it believes is appropriate.

Private versus Public Information

If you engage in a discussion related to ENTERPRISE, in addition to disclosing that you work for ENTERPRISE and that your views are personal, you must also be sure that your posts are accurate, not misleading, and that they do not reveal non-public company information. If you are in doubt, ask your supervisor. If you are still in doubt, don't post. Non-public information includes:

- Any topic related to the financial performance of the company;
- Information directly or indirectly related to the safety performance of ENTERPRISE systems or components for vehicles;
- ENTERPRISE Secret, Confidential or Attorney-Client Privileged information;
- Information that has not already been disclosed by authorized persons in a public forum; and
- Personal information about another ENTERPRISE employee, such as his or her medical condition, performance, compensation, or status in ENTERPRISE.

When in doubt about whether the information you are considering sharing falls into one of the above categories, DO NOT POST. Check with ENTERPRISE Communications or ENTERPRISE Legal to see if it's a good idea. Failure to stay within these guidelines may lead to disciplinary action.

- Respect proprietary information and content, confidentiality, and the brand, trademark, and copyright rights of others. Always cite, and obtain permission, when quoting someone else.
- Make sure that any photos, music, video, or other content you are sharing is legally sharable or that you have the owner's permission. If you are unsure, you should not use it.
- Get permission before posting photos, videos, quotes, or personal information of anyone other than you online.
- Do not incorporate ENTERPRISE logos, trademarks, or other assets in your posts.

If during your work you create, receive, or become aware of personal information about ENTERPRISE employees, contingent workers, customers, customers' patients, providers, business partners, or third parties, don't disclose that information in any way via social media or other online activities. You may disclose personal information only to those authorized to receive it per ENTERPRISE Privacy policies.

Option for More Restrictive License Terms

If you prefer to offer your Content on more restrictive terms, you may do so as follows:

- For content, you submit to a social network other than your own, label your submission with a full copyright notice, i.e., your name, the word "copyright" or symbol "©", and the year of first publication.
- By posting your Content using the Services, you are granting ENTERPRISE a non-exclusive, royalty-free, perpetual, and worldwide license to use your Content in connection with the operation of the Services, including, without limitation, the license rights to copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your Content, and/or to incorporate it into a collective work.

Attribution

When publicly displaying, publicly performing, reproducing, or distributing copies of your Content or Content as incorporated into a collective work, ENTERPRISE will make its best efforts to credit your authorship. You grant ENTERPRISE permission to use your name for such attribution purposes. You, likewise, agree to represent yourself accurately. You acknowledge that misrepresentation may lead us, in our sole discretion, to cancel your use of the Services and delete any of your Content.

Rules for Social Network Engagement

Social Networking is now the way of the world. Everything from personal communication, photo distribution, eCommerce, news dissemination, and political debates is now done on social networks. To that end, the IT Governance process needs to consider that. Rules need to be put in place on how an enterprise, its spokesmen, and employees interact and have social network engagement.

Understand the audience

Each social network has a different audience and disseminates information differently. Try out the applications - A first step is to see the features and functions of existing social networks. This includes:

- Blogger
- Facebook
- LinkedIn
- Twitter
- YouTube
- Wikipedia
- Buffer for distribution
- Others

If the technology group does not set rules and standards, the user community will take it upon themselves to integrate consumer apps into their work lives. This, in turn, can cause issues with the "social reputation" of the enterprise.

As a first step try out social networking with a low-cost pilot. Many open-source tools are widely available to experiment with. Another option is hosted applications which usually offer a small number of corporate licenses at a very low price.

Set Realistic Goal

Do not promise operational organizations and management that the enterprise's social network will do everything. Establish a pilot project with defined metrics. Be willing to walk away.

Set reasonable goals for user adoption and focus your initial deployment on a few groups that are eager for social networking tools. Establish pragmatic metrics and measure business value. This will be the basis for an ROI analysis for senior management's approval before rollout.

Do Not Let the Unknown Stop You

Many enterprises are wary of open social networks because they do not know what the networks will evolve to. Some executive management worries that employees will overdo the "social" aspects of these applications.

CIOs are tempted to police employee-generated content, either through monitoring or pre-approving posts. Resist that temptation; it will have a chilling effect on participation. Employees need time to grow comfortable with speaking up, sharing ideas, and participating in company-wide conversations. A social networking project will likely wither before it has a chance to grow if people fear the thought police.

Utilize Open Networks

CIO and CFO have a predilection to control and push to build gated networks, but that approach defeats the purpose of a social network.

The freer a social network is the greater the probability that it will evolve and grow. At the same time, security and compliance with mandated requirements need to be built in. That includes pilot programs.

Build a search capability

Build a Search Capability From day one – a poor index and search engine makes social applications less useful. A poor index and search engine make many social useful. A primary requirement is to have a strong "Google-type" search capability and road maps. Allow for user-generated feedback such as tags and content-rating systems, because the point of social networking in business is to let people provide input into the relevancy of content and people.

Include Enterprise data

Provide a way to integrate existing data but balance that with security and sensitive information policies and procedures.

Social Network Best Practices and Guidelines

The same principles and guidelines that apply to ENTERPRISE business activities apply to online activities. Also:

1. Follow ENTERPRISE policies and guidelines as published in all ENTERPRISE documentation.
    - If you have any confusion about whether you should post something on a social network, chances are ENTERPRISE's policies, procedures, and guidelines will provide guidance.
    - Know what proprietary, confidential, and sensitive information is. If you are still unclear on this do not post it until you seek the advice of management.
2. Do not comment on any legal matters or events that may put ENTERPRISE at risk.
3. Inform your immediate supervisor of all social network activities.
4. Identify yourself – name and, when relevant, role at ENTERPRISE – when your social network about ENTERPRISE or ENTERPRISE-related matters.
    - ENTERPRISE discourages anonymous postings on any social network or website on items that relate to ENTERPRISE, our business, or issues with which ENTERPRISE is engaged. We believe in transparency and honesty.
    - Use your real name, be clear about who you are, and identify that you work for ENTERPRISE.
    - Point out your vested interest in something you are discussing.
    - Protect yourself and your privacy. Be judicious in disclosing personal details
5. Write in the first person and make it clear that you are speaking for yourself and not on behalf of the ENTERPRISE. Use a disclaimer.
    - Make it clear that what you post is representative of your views and opinions and not necessarily the views and opinions of ENTERPRISE.
    - Place the disclaimer prominently on each social network post and/or web page.
    - Use a suggested disclaimer such as "The postings on this site are my own and don't necessarily represent ENTERPRISE's positions, strategies or opinions."
    - This standard disclaimer does not exempt ENTERPRISE managers and executives from a special responsibility when social networking. They must consider whether personal thoughts they publish may be misunderstood as expressing ENTERPRISE positions. A manager should assume that his or her team will read what is written. A social network is not the place to communicate ENTERPRISE policies to ENTERPRISE employees

6. Follow copyright, fair use, and financial disclosure laws.

    - Never quote more than short excerpts of someone else's work.
    - Provide a direct link to others' "work".
    - Never provide forecasts or financial data. This information is governed by laws including Sarbanes-Oxley and has very special disclosure requirements. Included are statements about an upcoming quarter or future periods or information about alliances, product and market development status, and applies to anyone including conversations with Wall Street analysts, press, or other third parties (including friends). ENTERPRISE policy is not to comment on rumors in any way. Do not deny or affirm them.

7. Exclude ENTERPRISE's and/or another's confidential or proprietary information. For example, ask permission to publish someone's picture or a conversation that was meant to be private.

8. Exclude references to employees, other individuals, contractors, clients, partners, suppliers, or firms without their approval.

    - Clients, partners, or suppliers should not be cited or referenced without their approval.
    - Never identify a client, partner, or supplier by name without permission, and never discuss confidential details of a client engagement. It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a client (e.g., Client ABC) so long as the information provided does not violate any non-disclosure agreements that may be in place with the client or make it easy for someone to identify the client.
    - Do not conduct business with a client on a social network.

9. Exclude ethnic slurs, personal insults, obscenity, and other disparaging comments.

    - Assume whatever you post can be taken in the wrong way by someone.
    - Look at all items you will post and see what could be taken out of context.

10. Show proper consideration for other's privacy and for topics that may be considered objectionable or inflammatory – such as politics and religion.

11. Don't pick fights, be the first to correct your own mistakes, and don't alter previous posts without indicating that you have done so.

12. Provide worthwhile information and perspective.
    - Social networks that are hosted on ENTERPRISE-owned domains should be used in such a way that adds value to ENTERPRISE's business.
    - Social networks that can adversely affect ENTERPRISE should be avoided. If you find such a social network, you must immediately inform your supervisor.
13. Respond to your errors, if you make an error admit it and correct your mistake quickly.
14. Don't let social networking interfere with your job and commitments to others.

Security Standards

The social network maintenance process that should be followed includes:

- Protect sensitive data.
- Protect encryption keys, user ids, and passwords
- Protect secure systems and applications
- Manage user ids to meet security requirements
- Restrict physical access to secure data paper and electronic files
- Regularly monitor and test networks
- Monitor all access to network resources and sensitive data
- Test security systems and processes
- Maintain an information security policy

BYOD Security

By adopting strategies that are flexible and scalable and taking advantage of new and upcoming security features, ENTERPRISE will be better equipped to deal with incoming challenges to their security infrastructure posed using employees' own devices.

- Follow the formal BYOD policies of ENTERPRISE
- Implement locking of the device after 5 minutes of inactivity
- Implement a remote wipe of the BYOD if the device is lost or stolen
- Limit the storage of sensitive and confidential information

Protect Sensitive Data

Standards and procedures include the following:

- Do not post sensitive data on any social network.
- Do not post customer information
- Do not post financial information about ENTERPRISE that has not been disseminated by the Chief Financial Officer of ENTERPRISE
- Redact sensitive data from documents that are provided to outsiders for whatever reason, and
- Utilize the most current working version of anti-virus,
- Validate that anti-virus is always running and producing logs that can be reviewed,
- Maintain and utilize current anti-virus definitions, and
- Never send sensitive data via email. If you must send sensitive data, do so in an encrypted file that is sent as an email attachment. Do not include the description of the encryption method and/or password in the same email.

Disaster Recovery and Business Continuity

Social media tools are pervasive and should be included in the disaster recovery and business continuity planning process. Social media spreads word of mouth, both good and bad. Plans need to use blogs, videos, and Twitter to rapidly spread information during a crisis, from earthquakes in China to Fires in L.A., to Hurricanes in the South, and now terrorist attacks.

Disaster Recovery and Business Continuity Plans need to be updated to:

- **Enhance Communication Plans**: Just as your enterprise has an existing communication plan (often a press statement from executive management to media) understand how to repurpose these messages and communication on social networks.
- **Experiment and Build a Base**: Enterprises should experiment with the tools the Department of Homeland Security offers and understand how to use these tools for disasters
- **Educate, Train, and build Awareness before an Event**: Companies as they test their DRPs and BCP should incorporate these social networks into the planning and execution processes. Companies need to indicate to the world what is an official channel, where people should go for news, and how each function plans to respond using these tools. These tools can help educate citizens on how to prepare for disasters, where to go for help, how to develop a crisis plan, and even basic life-saving medical techniques.

Best Practices in Managing Social Networks and Social Relationships

Social networks provide an opportunity to communicate electronically with both personal and business associates. Done properly they are a great new way to stay in touch or market.

- Create relationships to connect in a consistent manner
- Minimize low-value communications
- Group relationships to make it easier to track relationships
- Utilize multiple social networks to segregate relationships – utilize the right network for the relationship
- Ensure you have proper groupings
- Establish metrics to use in the following relationships
- Assess the impact of a change before you make it
- Document changes
- Keep communication flowing via Email
- Validate relationships are working both ways

Steps to Prevent Being Scammed by Social Media

With more companies moving to market via social media there now is a greater possibility that social media scams will impact and compromise your company. Here are some steps that Janco Associates has found that can minimize that risk.

- Implement a social networking policy for all individuals and devices that can impact the company's infrastructure
- Social engineering awareness training must be done constantly, not the typical annual training program.
- If it sounds like it is too good to be true, the odds are it is a scam
- Look to the outside to be aware of scams that others are facing
- Question suspicious behavior and communications.
- Report suspicious behavior and communications to the IT and HR management instead of sharing on social networks.
- Work devices should not be used for personal activities.
- Access to various types of data should be protected with separate and strong passwords.
- The network should be segmented to guard against scammers infiltrating a network segment simply because an employee with access to another segment was compromised.
- Learn from past mistakes of others. Reverse engineer, this same scenario in your own company to see if the scam could happen in your organization.

Appendix

Job Descriptions

Three (3) full job description is included with this policy template. It comes separately in its directory.

- Chief Experience Officer
- Manager Social Networking
- Social Media Specialist

Electronic Forms

Two (2) Electronic forms are included with this policy template. They come separately in their directory.

Internet and Electronic Communication Agreement

Social Network Policy Compliance Agreement

Protection from Ransomware, Phishing, and Whaling Attacks

Ransomware attacks are aimed at enterprises that need to have systems operational to function. Executives are most likely to be targets of a whaling attack. Phishing attacks are aimed at anyone with an e-mail address, whaling attacks target senior management at companies where knowing a top executive's password opens a back door to sensitive insider information. With private information becoming public via social networks, senior executives are being targeted via "whaling" attacks.

These whaling attacks are a form of personalized phishing, or spear phishing, aimed at senior executives or others in an organization that have access to lots of valuable or competitive information. While phishers generally go after consumers for bank account data, passwords, credit card numbers, and the like for financial gain, whalers most often target people who have inside information or can provide ongoing access to systems.

Whaling attacks are harder to detect than phishing expeditions. There's no obvious signature to detect as in phishing, such as seeing hundreds of copies of a phishing email enter your server. Whaling attacks are also hard to defend against because they often play on executives' feelings and sense of self-importance.

Steps that CIO should follow include:

Ransomware Attacks

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions on how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

There are several vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam - attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. If you want the technical details, the Infosec Institute has a great in-depth look at how several flavors of

ransomware encrypt files. But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.

In some forms of malware, the attacker might claim to be a law enforcement agency shutting down the victim's computer due to the presence of pornography or pirated software on it, and demanding the payment of a "fine," perhaps to make victims less likely to report the attack to authorities. But most attacks don't bother with this pretense. There is also a variation, called leakware or doxware, in which the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. But because finding and extracting such information is a very tricky proposition for attackers, encryption ransomware is by far the most common type.

Know what a whaling attack is

Watch for odd requests, links that don't make sense to normal communications, and attachments that are not generally sent by the purported sender. If you get an email that appears to be sent by a colleague but seems suspicious, check with the person to make sure he or she sent it. And keep in mind that some of the most common whaling techniques involve emails purportedly sent from one member of the executive management team to another.

In general, always be suspicious of unsolicited emails. Never click through links in an email message from someone you don't know -- unless you initiated the email exchange. You should be suspicious when an email message sender knows too much about you.

Inform your senior executives about whaling attacks and give them examples

No matter how busy executives might be -- or how much they resist going through security awareness instruction -- they need to attend training sessions regularly. They should be told what to look for in suspicious emails, as well as how to identify in-person whaling attacks, where an individual who might appear trustworthy gathers information over several months that can be used to access corporate systems.

Aside from training people on how to avoid being a whaling victim, reiterate the importance of protecting valuable data such as intellectual property. According to the 2011 Data Breach Investigations report said recently there have been more targeted attacks on specific types of data that aren't typically stolen in bulk, such as certain varieties of sensitive organizational data and intellectual property.

Conduct penetration testing and social engineering

How well did attendees of security training classes pay attention to what they heard? Why not find out by running some tests? Periodically called people in the organization at random to try to socially engineer them into giving up information they should not be sharing.

In addition to periodic testing, conduct individual consulting with people who are repeat offenders of security policy. There might be a root cause of why people are performing notable behaviors,

Use common sense with social networking

Facebook, LinkedIn, and other social networking sites have become valuable tools for building business contacts and for online collaboration and recruiting. But they're also places where whalers go to gather the information that they can use in attacks.

Some companies ban the business use of social networking outright. They block access to these sites from the corporate network. When people need access to social networking sites from work, they must first gain permission from the information security department.

For most organizations, blocking or curbing social media activity is not realistic. As websites such as LinkedIn recommend, don't link to people you don't know or trust whoever sends an invite, even if it sounds like a potential customer or business partner.

Be sensible about what you post: Not revealing too much information on the publicly visible portions of social networking profiles can help significantly. If an attacker can determine from someone's Facebook profile -- without being connected as a friend -- where they grew up, their marital status, date of birth, etc., they can craft a very appealing message and win over their confidence easily to act on the email link.

Practice safe browsing to avoid viruses and keystroke-capture programs

Keep your antivirus/malware detection software up to date, keep your browser updated to automatically block known attacks and known bad sites, separate work and play (consider using a separate browser for each), and if you must download content be sure to scan it for malware before running it.

Use security technology to help thwart attacks

Use digitally signed email which allows users to create their own trusted contacts and can increase the privacy of their emails. Other security tools, such as spam filters, firewalls, and intrusion detection and prevention systems, can help incrementally reduce the threat, he says.

To reduce the chances of being whaling victims, those in key roles need to recognize that they are potential targets and behave defensively.

Social Networking Best Practices

Twitter

1. Locate a good image of your enterprise's logo and have a good JPG file on your computer.
2. Decide how many accounts you want on Twitter.
3. Create a new Twitter account for each, fill out the profile completely and upload the most recognizable image of you or your company/product.
4. Find the Twitter account and follow it.
5. Look at the listing of followers and "follow" each of the other members.
6. As people follow you and your new Twitter accounts, take a look at their profile and follow them as well.

Keep your posts relevant and valuable

When someone "follows" you on Twitter, they have searched for a Twitter account name and clicked the "Follow" button. They will expect you to post relevant comments or announcements with that account. Since they will be seeing or reading your posts, you want them to expect a certain kind of value and receive that.

How many accounts?

So, you'll likely want two different kinds of Twitter accounts: one for yourself as an individual and another for the company or its major offering. For instance:

- @CompanyNameBCPManager is the Business Continuity Manger's communication
- @CompanyName is for the company's topic-specific comments

Naming your accounts

When someone searches for you on Twitter, you want your account name to match what they would search for. It is unlikely your customers and other stakeholders would know your specifics, so use account names that are easy to find

- @CompanyNameBCPManager is the Business Continuity Manager's communication
- @CompanyName is for the company's topic-specific comments

Profile

Once you have created one or more Twitter accounts, set up the profile on Twitter to include a description of yourself or your business as well as a link to the relevant page on your website.

When people search for Twitter accounts or consider following someone they've found, your profile page is what tells the story about you and suggests what kind of value they will get when they subscribe to or follow you.

LinkedIn

- Create a new account on LinkedIn and edit your profile to describe you, your history, and your business
- Seed your connections by uploading your email contacts
- Review each new connection's connections for people you know and invite them to
- join your LinkedIn network
- Create a profile for your company.
- Link your blog to the LinkedIn profile.
- Join relevant groups.

LinkedIn started as a simple directory of business people and has grown into a powerful tool for finding people and, more importantly, finding answers to your business questions. Conversely, an individual can establish themselves as an authority and the company as the "answer" if they participate in the Questions and Answers sections of LinkedIn.

Finding connections

The networking part of LinkedIn is useful for recruiting or prepping for a sales call or for locating the right person within a company or community. You can access other people's information so long as you are connected to them in some way.

seed your connection list by uploading the address book from your email program. LinkedIn will look for other LinkedIn members with those addresses and start the process of connecting them to your new account.

Once the other party has confirmed you as a connection, you should view their list of connections and use the "Add To My Network" feature for everyone you recognize.

Linking to groups

Another strong way to make connections and join pertinent discussions is to join groups of LinkedIn members. Once joined, the individual can read and participate in the online discussion forums on LinkedIn specific to the group.

Adding a company profile

LinkedIn is the ability to add a profile for your company. This will help with searches and LinkedIn members will discover how to use this information quickly.

You'll want to be the first to add your company to the profiles on LinkedIn so you'll be in control of the entry.

Adding a blog feed

Once there is a LinkedIn profile, you can add a link to your blog and have LinkedIn automatically add an announcement of your new blog posts to your LinkedIn profile. That means visitors to your LinkedIn page will see your most recent blog entries.

Blog

- Decide on a topic and post each week
- Pick a searchable, relevant name and create a new account on WordPress or
- Blogger.com
- Edit your profile to describe you and the company and point back to your website
- Post a new entry at least once a week
- Announce the blog as often as you can and announce each blog entry on your other social networking and Internet marketing sites.

For a blog to "work", people to read your blog regularly. They must have a reason to come back over and over. That translates into "you need to post valuable information and/or opinion, and do so regularly." You could create a blog that features your opinion on your industry or your product line. Or you could create a company blog that talks about how your product or service helps your customers. Or you could create a blog about how products like yours help businesses or consumers. There are many topics or perspectives which would interest your customers and prospects. You'll have the most success if you choose something that has great value for the reader and for which you have great enthusiasm and interest.

Create a blog account somewhere else

You'll want your blog to be hosted somewhere other than on your website so Google "sees" it as an external source that points back to your website. That makes it easy to create a blog.

Use WordPress or Blogger to create a free blog. Pick a name that conveys your name, your company name, or the product/industry you serve. The title of the blog needs to be attractive to human readers as well as to Google and its search for keywords to match user searches.

Prepare your blog profile

Similar to the Twitter profile page, a blog profile needs to identify you, your company, and the product and services you offer. The words you use to describe what you do will be cataloged by Google and added to its database of keywords.

Be sure to point readers directly from your blog profile back to your website. You may even want to point them to a specific part of your website, for instance, the landing page for the product which your blog talks about most, instead of the more generic home page.

Add content regularly

To get visitors to return to your blog each week, you'll need to add content regularly. You may find it difficult to make time to think of a topic, write about it and post a blog entry regularly.

Try picking out a specific day a week, schedule a recurring meeting with yourself on that day at the same time, and devote that time to writing a short blog entry. If you need ideas on what to write about, bookmark this link and choose one question from the list to answer and post each week

Announce your blog

Communicate to your customers, your staff, your friends, and your peers about your blog. Ask them for feedback, and ask them to leave comments. The more times you tell interested people about the blog, the more visitors and regular readers you will gain. If you have a newsletter, remind readers of each issue. Put an announcement and a link all over your website. Add a signature line to your outgoing email directing people to your blog.

Tell everyone you are writing

Once you have created a Twitter account, a Facebook account or page, a LinkedIn account, or similar, connect your blog to these services so each new blog entry results in an announcement on Twitter, Facebook, LinkedIn, and beyond.

Most modern, popular services like this have a place in the settings or applications where you can give the URL or RSS address of your blog. That service then automatically announces the fact you've made a blog post, increasing the traffic to your blog and the number of readers.

For the services where there is no auto-post-announcement, just remember to follow up on your blog posting with a quick "hey, I just posted this useful entry on my blog" announcement everywhere else.

What's News

2022 Edition

- Added job description for Chief Experience Officer
- Updated all the included electronic forms
- Updated all the included job descriptions

2021 Edition

- Added strategy on how to implement enterprise social networking
- Added materials on Ransomware attack protection
- Updated materials on phishing and whaling attack protection
- Updated all the included electronic forms
- Updated all the included job descriptions

2020 Edition

- Updated all the included electronic forms
- Updated all the included job descriptions
- Updated to meet the latest mandated requirements

Version 2.2

- Added job description for Social Networking Manager
- Added a section on enterprise rules for social network engagement
- Updated to meet the requirements for CaCPA

Version 2.1

- Added Internet and Electronic Communication Agreement electronic form
- Updated Social Networking Policy Compliance Agreement electronic form
- Updated Social Media Specialist job description
- Updated policy to meet EU compliance requirements

Travel, Laptop, PDA, and Off-Site Meeting Policy

2023 Edition

Janco Associates, Inc.

License Conditions

Table of Contents

Travel, Laptop, PDA, and Off-Site Meetings

Protection of ENTERPRISE data and software is often complicated by the fact that it can be accessed from remote locations. As individuals travel and attend off-site meetings with other ENTERPRISE employees, contractors, suppliers, and customers - data and software can be compromised.

It is the responsibility of all users, data owners, and data managers to ensure that adequate controls exist per the Internet and Information Technology Security Manual or special requirements as established by the Audit Department or the Internet and Information Technology Security group. Enforcement of these controls is imperative to provide the best environmental security possible.

In addition to that, the following procedures should be followed.

Ongoing monitoring and evaluation of this policy are critical to the success of our computing environment. Clear processes and ownership of monitoring the policy consistently enable the identification of policy elements that are working well and others that are not working. If this policy causes disruption in productivity in the organization, it needs to be evaluated to understand what the problem is.

Laptop and PDA Security

- All laptops and PDA devices (Palms, Blackberry, etc.) that are linked to ENTERPRISE information are the property of ENTERPRISE. All available forms of security are to be applied to these devices including and not limited are: passwords, encryption, biometrics, lo-jack, and auto-locking.
- The use of automatic logins is prohibited. Use of utilities that bypass or save passwords and log-on sequences is prohibited. Data on Laptops and PDAs must comply with the Sensitive Information policy of ENTERPRISE.

BYOD Security

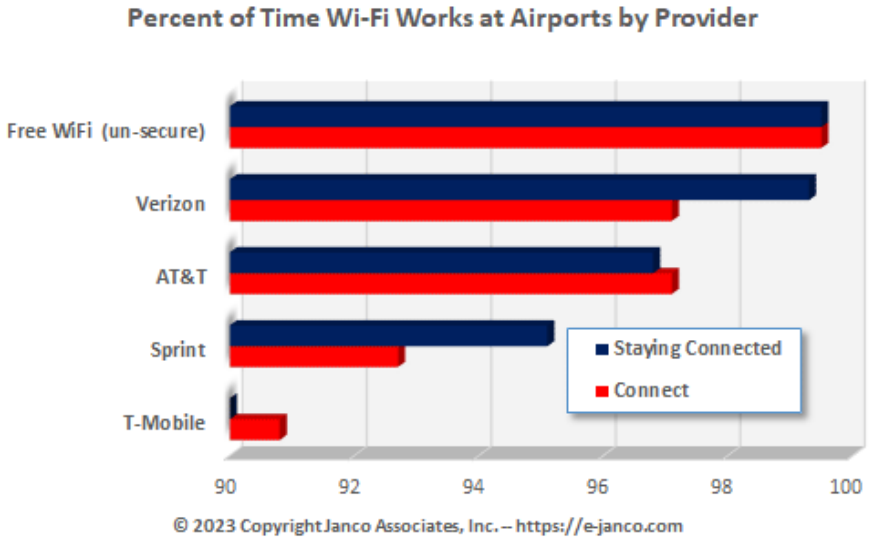
By adopting strategies that are flexible and scalable and taking advantage of new and upcoming security features, ENTERPRISE will be better equipped to deal with incoming challenges to its security infrastructure posed by the use of employees' own devices.

- Follow the formal BYOD policies of ENTERPRISE
- Implement locking of the device after 5 minutes of inactivity
- Implement a remote wipe of the BYOD if the device is lost or stolen
- Limit the storage of sensitive and confidential information

Service Provider Selection

The service provider selected by individuals can have an impact on the costs incurred both by the individual and the enterprise. For example, when traveling access to Wi-Fi can become expensive because of poor coverage by the provider. In a survey of the availability of Wi-Fi at airports, conducted by Janco Associates, Verizon provided over 99% availability for Wi-Fi. At the same time, T-Mobile provided less than 90% availability. Granted this is only a small sample but it shows that CIOs need to understand where their users are and then look to see what the service levels are for those areas.

One word of caution, most airports now provide "free" un-secure Wi-Fi. This connection should be avoided as it is an easy entry point for hackers. At the very least, when connecting through un-secure Wi-Fi, a VPN client should be used and have malware protection installed on the device used.



Wi-Fi & VPN

- The use of public Wi-Fi networks without ENTERPRISE-approved encryption is prohibited. Every Wi-Fi device needs to conform to the network security configuration standard. Passwords and log-on sequences should never be transmitted in a clear (unencrypted) text format.
- Access to ENTERPRISE VPN (Virtual Private Network) is limited to those individuals and devices that have been approved by ENTERPRISE.

Data and Application Security

- Do not take your PC on a trip unless it is necessary. If you need to take a PC, minimize the data and programs that are on the PC.
- Follow company procedures and practices to minimize ransomware exposure threats
- Use unique usernames and passwords for files on the PC.
- Use an external storage device for data and programs. The external storage device data should be encrypted.
- Use biometrics and other techniques, such as removable storage devices (when possible). This should help to limit risks to ENTERPRISE if the PC is lost or stolen. Do not store the external storage or key device with the PC.
- Do not automatically save usernames and passwords on the PC.
- Do not leave your PC, PAD, or printed documents unattended. If you have to leave them in your hotel room, be aware that it can be a major breach of security – see if there is a safe that you can put them in.
- When attending an offsite meeting, the organizer should provide a facility where you can check your equipment and reports which is secure and guarded.
- When using remote printing send a test page before you send secure data. Be in the location where the printer is printing. If there are any paper jams retrieve all of the pages. After the jam see what comes out next.
- When you are finished with a report that contains secure data, keep it with you until it can be disposed of properly.
- At the end of the trip consider sending sensitive reports back to your office via express delivery services like FedEx or UPS.
- When sending a fax with secure data via a service, keep sight of the source document and validate it was sent to the correct fax machine.

Minimize Attention

- When traveling, bags or luggage containing equipment, such as computers and important ENTERPRISE documents, should not attract attention. For example, they should not have labels or business cards on them which show ENTERPRISE's name on them.
- When on an airplane or train do not expose documents or computer screens so that anyone can read them.
- When traveling with an associate, speak in muted tones and use code words for critical data, names, and processes.
- When checking into hotels, when possible, do not include ENTERPRISE's name as part of the registration.

Public Shared Resources – Wireless and Shared Computers

- When using wireless networks use enciphering to minimize the "over the air" capture of data that is being sent or received. Issues include:
  - ✓ There is no clear owner of wireless – even internally, multiple people think that they own it, but don't have all the tools necessary to manage it
  - ✓ Employees don't follow the policy and end up going through the process to procure whatever they want and their managers support it.
  - ✓ Productivity has come to a standstill because employees don't know how to get devices, who to call for support, or how to use their new devices. The distraction of all of the chaos and the soft-dollar cost of lost employee productivity is huge.
  - ✓ The enterprise has a policy but the executives do not conform (frequently C-Level executives are the biggest offenders).
  - ✓ After writing a policy and trying to implement it, wireless still causes too many issues and distractions within the organization.
  - ✓ The enterprise offers the latest and greatest devices as a perk to employees and feels it cannot take that away. It prides itself on having employees use cutting-edge technology.
  - ✓ Employee turnover regularly results in proprietary information leaving the company on non-company-owned phones.
- When using a shared computer do not access secure data and try to not use common passwords. It is a good practice to obtain a unique user id and password for each "trip" that is deactivated at a time certain.

Off-Site Meeting Special Considerations

- Do not have ENTERPRISE's name on posters or electronic messaging boards available to the public when holding an off-site meeting. Use "Private Meeting" or a bogus name or the name of the person who is leading the meeting as a way to identify the location.
- When holding off-site meetings, and discussing secure data, consider having "white noise" like music which would minimize the ability of some to listen in.
- Verify that there are no cameras (with or without audio) in the facility's meeting rooms and gathering places that can capture the events.
    - ✓ If the meeting room has windows set the projection equipment up in such a way that no one outside can see the screen
    - ✓ If the meeting room is adjoined to one that has no soundproofing, see that your meeting cannot be heard in that room – use white noise if necessary.
- When the meeting is in session, do not allow anyone of the attendees to use their cell phones or recording devices.
- There should be some assigned to the door and they should monitor this.
- Name tags and/or security badges should be provided to each attendee. These should be worn by everyone and used as an admission pass to the meeting.
- Monitor the individuals from the off-site faculty who are in your rooms during the actual meeting.
- Facility support personnel should have ID badges with a photo.
- Facility support personnel should not use any cell phones, PADs, or related technology in their possession when they are in your meeting while it is in session.
- When confidential or secure data (posters, whiteboards, notebooks, or documents) is left in the meeting room while the meeting is not in session the room should be locked and monitored by the security staff of the off-site facility or ENTERPRISE's personnel.
- After the meeting is over clean up the room and leave no sensitive or confidential information in the meeting room. Consider having a cross-cutting shredder to destroy data in place.

Pandemic Issues

- **Safety and well-being.** Priory should be people – That includes company staff, company partners suppliers and their staff, their staff, and customers/clients. Their safety and well-being always come first, and they are best informed with factual data.
- **Business impact.** Understand the business impact of any decisions. For example, if a meeting or event is canceled what will the social, scientific, or economic impact be acceptable? What happens if we continue with the meeting or event and participation is reduced? Will this have an impact greater than canceling? What alternatives could be considered? Change of destination, date, or including a virtual element?"
- **On-site risks.** Risks are typically a combination of the severity of impact vs. the likelihood of different scenarios. Use a risk assessment matrix to plot, identify, and rank risks to determine and decide on appropriate responses. In times of heightened risks, establish a quick response team.
- **Communications.** It is essential for meeting and event providers and the company to work closely together. This ensures that the broad view and all possible issues and scenarios can be considered and addressed. Continued communication with all stakeholders is also a core part of the approach to ensure people have regular updates and are aware of who to contact in case of questions.

International Travel Best Practices

- If it's not necessary, don't travel with it. Whenever possible, arrange to use loaner laptops and handheld devices while traveling
- Use a SIM card for Smartphones
- Apply full encryption, picking a long, complex password
- If you are bringing a laptop with you, make sure you have the proper plug adapter
- Install a host-based firewall, and configure it to deny all inbound connections
- Disable file, printer sharing, Wi-Fi, and Bluetooth.
- Update all software immediately before travel - Disable automatic updates while you travel
- Always clear out the browser cache before you leave
- Backup your computer before you leave
- If you are bringing private data, not on a computer, copy the data onto an encrypted USB memory device - or the cloud
- Change the password for your account's email, Gmail, Facebook, etc.
    - ✓ Utilize complex passwords - Assume the workstation or medium will be lost or stolen
    - ✓ Memorize the password, or keep it in a secure location on your person
    - ✓ Password protects the login and requires the password after the screen-saver
    - ✓ NEVER set the browser to remember passwords
    - ✓ After returning to the home base change all passwords

Remote Computing Best Practices

The following best practices should be followed for all remote computing

- **Test connectivity before the trip**. Have a checkup procedure that tests the connectivity of the laptop which is disconnected from the in-house network.
- **Turn off ad-hoc networking features.** Default settings in Microsoft Windows allow a notebook computer to look for any available wireless networks. Because you need to prevent the sharing of corporate information with strangers, you should insist that your employees disable the ad-hoc networking feature before they use a public hotspot.
- **Turn off file sharing**. Microsoft Windows by default enables its users to share files with strangers. You'll want to turn that feature off before they hit the road.
- **Validate that nobody is looking over their shoulders at hotspots and on airplanes**. Thieves can steal passwords just by watching someone type those passwords.
- **Use a VPN**. A virtual private network creates a tunnel between the mobile device (smartphone or computer) and the corporate network. Implement a policy requiring the use of VPN software for remote access to the corporate server. A VPN virtually guarantees that nobody can intercept sensitive information on the company's server. Most commercial hotspot providers support VPNs. Public libraries often do not.
- **Use a firewall**. With a Wi-Fi hotspot, a group of strangers is sharing the same IP subnet. Odds are most of these strangers have no ill intentions, but they might unknowingly have malware or viruses on their computers. Thus, they might unknowingly infect the computers of those around them. Installing (and running) firewall software will help to prevent successful attacks from both on and off the subnet. A firewall should block attacks and send an alert when it detects any unwanted attempts to connect to your employee's computer.
- **Install and use antivirus software**. Should a virus get through, antivirus software will detect and thwart it - provided the software recognizes the virus. New viruses are created daily. For that reason, most antivirus software companies provide frequent updates to their software. It's up to the user to go to the vendor's Web site to obtain the updates. This should be done at least once a week.
- **Encrypt all portable media devices**. Confidential and sensitive information on all portable media devices including Smartphones, laptops, USB storage devices, and tablets should be encrypted so that if they are lost, confiscated, or stolen that no enterprise or personal data is compromised.
- **Encrypt any folder that contains sensitive data**. Securing the data that resides on a device is a safety issue any time that the device leaves the office. Employees may be lax about encrypting the contents of their computers, but they need to know that sensitive data means more than financial information and social security numbers. Sensitive data include the folder in which they store all their network passwords.
- **Update the computer with the latest operating system patches**. Software vendors regularly send out patches to fix problems - including security problems. Typically the system alerts users to new patches with a little explanation point via a popup or in the right-hand corner of the screen. Installing these patches is generally a matter of just clicking on that exclamation point.

- **Validate that the device is connecting to the correct network**. Employees using a hotspot should make sure that their notebooks or handheld computers are connecting to the hotspot - and not to some other Wi-Fi network.
- **Use secure web pages**. Watch for "https…" in the Web address or a logo that looks like a gold lock in the right-hand corner of the page. This means the browser is using SSL for server-side authentication. If the connection doesn't include a log-in page, the computer is likely connected to the wrong network. At hotspots that charge a usage fee, avoid entering your credit card information into a site that does not employ SSL. If your employees are conducting any sensitive business transactions via the Web, they should try to use only Web sites that employ SSL.
- **Turn off the wireless, Bluetooth, and radio when you don't need them**. Disabling ad-hoc networking should prevent a computer from connecting to wireless networks indiscriminately.

Electronic Meetings

Individuals involved in conducting meetings are moving to more dynamic and efficient ways of working. This has become increasingly important as companies hold more meetings and managers require ever-increasing levels of information. Add to this the number of individuals who work away from the office, there is a greater need to have meetings that are attended by remote users.

Typically, the meeting manager invites the participants to a meeting via email. The meeting can be held with both participants who are in the same room -- along with audio and visual displays that can be used in the course of the meeting. Remote meeting attendees participate primarily through their keyboards, typing responses to questions and prompts from the meeting host or via audio-visual input (in computer camera and speaker) and output display on a computer, tablet, or smartphone.

Best Practices for Electronic Meetings

Achieving that initial buy-in for electronic meetings is usually the most difficult part of the process but, even with the support of management, there is still work to be done. The following best practices, when followed, facilitate the effectiveness of this meeting process.

- Have an agenda that is available to all attendees before the meeting - a concise description of the off-site: objectives, expected results, and prospective attendees.
- Have a common secure location where share documents are available to all attendees – this is where minutes and meeting summaries will be posted
- Have a process to validate that the devices in use by users will work with the electronic meeting application
- Test the meeting technology with all attendees well in advance of the meeting. This includes sending a link to the client application so the attendees can test to see if they have it installed, audio can be heard and sent, and that video can be seen and sent with their computer.
- Be aware of the time zones that meeting attendees are in
- Have a specific start time and follow it
- Have a dress code including background for an electronic meeting
- Send an electronic invitation that requires a confirmation and put the meeting on the electronic calendars of all attendees
- Record the meeting and comments for others to review if they are not able to attend – Post the video on a common secure location
- After the meeting post a summary of the meeting including the next steps, tasks assigned, and when the next follow-up meeting will take place.

Appendix

Job Description

Four (4) Full job descriptions are included with this policy template. They come separately in their directory.

- Chief Experience Officer
- Chief Mobility Officer
- Manager Help Desk Support
- Manager Telecommuting
- Manager WFH Support

Electronic Forms

Four (4) Electronic forms are included with this policy template. They come separately in their directory.

- Mobile Device Access and Use Agreement
- Mobile Device Security and Compliance Checklist
- Privacy Policy Compliance Agreement
- Telecommuting IT Checklist
- Telecommuting Work Agreement
- Work From Home IT Checklist
- Work From Home Work Agreement

Revision History

2023 Edition

- Updated to meet the latest compliance mandates
- Updated all included forms
- Updated all included job descriptions
- Added 1 job description
  - Manager Work From Home Support
- Added three (3) electronic forms
  - Telecommuting Work Agreement
  - WFH Work Agreement
  - WFH IT Checklist

2022 Edition

- Added four (4) full job descriptions
  - Chief Experience Officer
  - Chief Mobility Officer
  - Manager Help Desk Support
  - Manager Telecommuting
- Updated all the electronic forms
- Added materials for remote operations

2021 Edition

- Updated all the electronic forms
- Added materials for Pandemic operations
- Added material for Ransomware

2020 Edition

- Added materials for Airport Wi-Fi and un-secure Wi-Fi
- Updated to meet the latest compliance requirement
- Updated all the electronic forms

Wearable Device Policy

2023 Edition

Jancoo Associates, Inc.

License Conditions

Published by: **Janco Associates Inc.**
Park City, UT 84060

Email – support@e-janco.com

Printed in the United States of America

Table of Contents

Wearable Device Policy

Overview

The purpose of this policy is to define standards, procedures, and restrictions for wearable devices that can capture, display, and or broadcast video, audio, WiFi data, and GPS location presenting new challenges for the enterprise.

There are clear benefits and risks to these devices in the workplace.

- They can be used for alerts and notifications as pagers and smartphones. Wearers can see the alert, and in many cases respond to it, while continuing to do whatever it is they were doing, even if they were in a meeting.
- Drivers, warehouse workers, and others who use both hands during work will benefit enormously. Wearable devices essentially give them the basic tools of a white-collar worker sitting at a desk as they are in the factory or the field.
- Images, recordings, and data can be transmitted to a location where others can direct the wearer to perform actions
- It will prove to be a benefit to the visually impaired and other disabled employees.

There are also definite risks associated with this technology when it is used with the expressed consent of the enterprise in locations where sensitive, personal, and or confidential information is located.

The policy applies to any device that could be used in such a manner, even when the equipment is not approved, owned, or supplied by ENTERPRISE.

Policy

Use of these wearable devices is allowable under the following conditions:

- The privacy and confidentiality of Enterprise facilities, systems, information, property, employees, guests, suppliers, and customers are maintained.
- Devices will not be used in any manner that compromises any individual or processes at enterprise locations.
- If the device is enterprise-owned and approved, it is not to be used away from enterprise locations unless it is specifically authorized by the enterprise.

There can be limited personal use of the device:

- Imposes no tangible cost to ENTERPRISE;
- Exposes ENTERPRISE to any liability or risk;
- Does not unduly burden ENTERPRISE's computer or network resources;
- Has no adverse effect on an employee's job performance?

Upon entry in any location noted with a sign that Wearable Devices are not permitted, the device should be removed and powered off. This includes facilities that are open to the public,

All users shall be required to acknowledge receipt and understanding of all regulations governing the use of Wearable Devices and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with ENTERPRISE policies.

Upon an employee's termination (voluntary or involuntary) any employee-owned Wearable Devices device is to be provided to their supervisor to ensure that all company-owned data (i.e. contacts, emails, files, etc.), applications, and network access information and tools are removed.

Violations of law may result in criminal prosecution as well as disciplinary action by ENTERPRISE.

Wearable Device Policy Requirements

The policy of ENTERPRISE is that these users must follow ENTERPRISE policies and procedures to support the management, tracking, securing, and supporting of these devices, just like they do for any other devices.

Specifically, the policies that apply to these types of devices are:

- Security best practices for Wearable Devices, including the use of multilevel passwords and device certificates, and the ability to remotely wipe the device if it is lost or stolen.
- Utilize tiered access to network resources to secure critical data and applications.
- Comply with device recordings and application delivery mechanisms.
- Synchronize the Wearable Devices applications and recordings to the corporate network at least weekly or whenever connected to ENTERPRISE's network.
- Create an enciphered backup of the Wearable Devices applications and recordings on a schedule that is approved by the CIO (Chief Information Officer)

Policy Definitions

The following are definitions that apply to this policy:

- **Wireless Network** - An connection point that allows two or more computers, to communicate, (enabling file sharing, printer sharing, internet connection, etc.), using standard protocol but without the use of network cabling and typically outside of ENTERPRISE's control
- **Employee** - An employee, contractor, associate, and others who work away from his/her central workplace either at home or at another ENTERPRISE-designated or approved remote work location utilizing a BYOD.
- **Wearable Devices** – A device that an employee or individual (on a property that is controlled, owned, leased, or used by the company) wears that has a camera and/or recording ability. With WiFi or cellular access, data can be transmitted and received on the device.

Access Control

- The CIO and Information Technology group reserve the right to refuse, by physical and non-physical means, the ability to connect Wearable Devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the enterprise's systems, data, users, and clients at risk.
- WiFi access is at the discretion of the enterprise and is governed by the overall security policies of ENTERPRISE.
- In addition to signage prohibiting the use of Wearable Devices ENTERPRISE reserves the right to jam WiFi and cellular access for Wearable Devices in areas where ts does not want the devices to be used. This is especially true with GPS. The default on many devices is to record and transmit the location. GPS should be turned on ONLY if required.
- ENTERPRISE reserves the right to install "self-destruct" code on the device which can be activated remotely or when a breach or other event occurs. ENTERPRISE is NOT responsible or liable for any damage or inconvenience that this can cause to the Wearable Devices or its owner. Also, the user of the Wearable Devices is prohibited from altering or removing this code without the prior written approval of their supervisor. If they do so they are then subject to immediate termination.
- ENTERPRISE reserves the right to audit any Wearable Devices device used on any of its premises or worn by its employees, suppliers, customers, guests, and others. Refusal to submit to this audit is grounds for immediate termination and or ejection from the facility.
- Before initial use on the enterprise property, all Wearable Devices must be registered with the manager they report to. That manager should communicate the use of that device to Information Technology which maintains a list of approved users and devices. Devices that are not on this list may not be confiscated or the user removed from the enterprise facility.
- End users who wish to connect such devices to non-enterprise network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet the enterprise's established IT security standards.
- All devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) can be electronically inspected by ENTERPRISE. Devices that have not been previously approved are not in compliance with ENTERPRISE's security policies or represent any threat to the network or data will not be allowed to connect.
- Wearable Devices may only access the enterprise network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required.
- Wearable Devices will access the corporate network and data using Mobile VPN software installed using procedures approved by or installed by IT.

Security

- Employees using Wearable Devices and related software for network and data access will, without exception, use secure data management procedures.
- Wearable Devices must be protected by a strong password, and all data stored on the device must be encrypted using strong encryption. See ENTERPRISE's password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All users of Wearable Devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by ENTERPRISE's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.
- Passwords and other confidential data as defined by ENTERPRISE's IT department are not to be stored unencrypted on Wearable Devices and their recordings.
- Any Wearable Devices that are being used to store ENTERPRISE data must adhere to the authentication requirements of ENTERPRISE's IT department. Also, all hardware security configurations (personal or company-owned) must be pre-approved by ENTERPRISE's IT department before any enterprise data-carrying device can be connected to it.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with per ENTERPRISE's security policy.
- Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.
- ENTERPRISE reserves the right to remotely wipe or copy any ENTERPRISE data on Wearable Devices that connect or attempt to connect to the network. This includes but is not limited to emails, contacts, business records, financial data, presentations, operational data and metrics, applications, and other data.
- In the event of a lost or stolen Wearable Device, it is incumbent on the user to report this to IT immediately. The device will be remotely wiped off all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.
- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both corporate-owned and personal mobile devices being used within the company premises.

Help & Support

- ENTERPRISE's IT department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of ENTERPRISE's IT department. This includes, but is not limited to, any reconfiguration of the mobile device.
- IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the enterprise network.

Creating a Wear Your Own Device Strategy (WYOD)

To get a head start on developing a wear-your-own-device (WYOD) strategy here are a few best practices to follow:

- Adjust the policy to combine restrictions with geo-fencing. IT can disable Bluetooth between wearable devices and IT-managed smartphones or tablets, either altogether or in high-risk areas.
- Use application blacklists to disable wearable-specific apps on managed smartphones. The IT function has several resources available to prevent users from sharing business data in personal apps specific to their wearables.
- When wearables lack enterprise-grade authentication, IT can use WLAN access control lists and intrusion prevention systems to block or allow enterprise network access to business wearables.
- If the organization allows WYOD, consider using authentication such as biometrics, proximity, and geo-fencing. These approaches are useful for enabling the device itself and for using wearables as an authentication token to unlock or start other business resources.
- Analyze network traffic to detect and measure the workload that wearable-generated data streams create. However, employers may want to avoid logging wearable device traffic too extensively, given that it often includes personally identifiable information.
- Use wireless intrusion prevention systems (WIPS) to detect and report irregular connections and potential attacks that could exploit business wearables. As with any new consumer electronics, wearables are likely to harbor at least a few vulnerabilities, and it's important to identify and address any low-hanging fruit
- IT can use regular processes to assess and enroll devices, provision security policies, applications, and data containers, and apply actions such as finding and wiping when business wearables are lost or stolen. Craft custom policies for these devices to balance risk and usability, and work with early adopters to refine those policies for future use.

Enterprise Mobile Device Infrastructure

- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.
- The end-user agrees to and accepts that his or her access and/or connection to ENTERPRISE's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains ENTERPRISE's highest priority.
- The end-user agrees to immediately report to his/her manager and ENTERPRISE's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
- Every Wearable Devices user will be entitled to a training session around this policy.
- A Wearable Devices user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

Wearable Device Infrastructure

- In all cases, all data, applications, user ids, passwords, and sensitive information will remain the property of ENTERPRISE.
- The employee will comply with all backup, record retention, security, sensitive information, business continuity policies, and procedures of ENTERPRISE.
- Under no condition shall any individual (especially children) utilize any Wearable Devices or another device that contains ENTERPRISE data.
- When employees are authorized to use their equipment, ENTERPRISE does not assume responsibility for the cost of equipment, repair, or service.
- Upon termination of employment, the individual grants the company the right to physically inspect the device to validate that all company data and intellectual property has been removed.

Disaster Recovery

The individual is responsible for the recovery of the applications and data on the device. The company will provide processes that can be used to restore company data, intellectual property, and applications.

The device is the property of the individual. If it is destroyed, lost, or stolen the individual is responsible for its replacement. The company has the right to create an image backup of the device but is not obliged to do so. The individual is obligated to notify the company when there is a change in the status (destroyed, lost, or stolen) so they can take appropriate action to deactivate the device and remove it from the approved list of devices that can interact with the company's network and data.

Backups

IT will provide a mechanism for users to back up their personal electronic data on. IT will assist users having problems with backups. However, IT is not responsible for backing up personal data such as music, movies, etc. Backing up personal information is the users' responsibility. IT has recommendations on how to best accomplish backups of personal information.

Public cloud backup such as iCloud is prohibited for all recordings and company-sensitive and confidential information.

Intellectual Property

The intellectual property contained on the personal device should be backed at least weekly and more frequently, such as daily or twice per day, based on the amount of updating that is done via the device. It is recommended that an automated backup tool is used for this. All data backed up to the cloud should be enciphered and password protected with a "strong" password.

Wearable Device Physical Device

Enterprise fully supports hardware and software problems on Wearable Devices as configured by IT. To provide this support, users, are required to update their tablets as required by the IT department. IT reserves the right to disconnect any Wearable Devices from the enterprise network if policies are not adhered to by users.

Security

All Wearable Devices should implement security procedures that require passwords to use the devices. Also, this should include activation of the self-destruction of all data if the password is entered in error more than 5 times.

The "FIND ME" application should be activated.

Supported Problems

IT will support hardware and software problems on the Wearable Devices as configured.

This means we will support the software that comes with the system from IT. IT will not support software that may be added by users.

Internal Network Access

Computers on the enterprise's network must adhere to all IT policies. If you do not meet these policies you can still get Internet access, as allowed by the enterprise, but you will not get access to enterprise servers that host network data storage and enterprise sensitive and confidential information including enterprise email.

Repair Procedure

Some software and hardware problems may require the IT department to wipe out the current installation of the operating system and reload the Wearable Devices' original configuration. This will result in the loss of data and any programs installed which are not part of the original configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their devices.

Upgrade Procedure

Upgrades to a new operating system will be applied by removing the existing installation and replacing it with the new operating system. This will result in the loss of data and any programs installed which are not parts of the configuration. Users are responsible for backing up any personal information and reinstalling any software they added to their tablets.

Patching Policy

As with all networked computers, regular patches to the Operating System and other applications will be installed remotely.

The IT department reserves the right to scan Wearable Devices remotely and apply patches as needed.

Wearable Devices missing important patches will be patched.

Ownership of device

Organizations face the legal question of who needs to own the device, though the concern isn't exclusive to them. The underlying issue concerns when ownership is necessary to gain management control. But more conservative organizations often decide they need legal ownership of the device.

The result has been three different approaches to handling ownership:

- **Shared management**. The organization's policies boil down to "if you access business resources from a personal device, you give us the right to manage, lock, and even wipe that device, even if you end up losing personal data and apps as a result for both parties.
- **Corporate ownership and provisioning**. The organization buys and owns the device, even if it allows nonbusiness use on it. Employees who do not like the phone service on such devices (they may not get free minutes when calling family members and friends) are free to carry a personal device as well that has no corporate access.
- **Legal transfer**. The organization buys the device from the user. In some cases, that ownership is permanent.

Ownership of data

It used to be that in the United States, you could reasonably assume that personal information communicated through cellphones and other such devices is considered private to the employee, based on various court cases and a set of laws called the Stored Communications Act. The key to that privacy was that the data was stored by a third party (a telco or Internet service provider), not by the company, which would have access to rights to whatever is stored, such as on its email servers. Essentially, the Stored Communications Act extended Fourth Amendment protections of a person and his or her property to that person's electronic data even when stored on "neutral" property (that is, a telco's or ISP's servers).

Employees have no privacy rights for what's transmitted on company equipment, but employers don't necessarily have access rights to what's transmitted on employees' own devices, such as smartphones, tablets, and home PCs. Also unclear are the rights for information that moves between personal and corporate devices, such as between one employee who uses her own Android and an employee who uses a corporate-issued iPhone.

This confusion extends to trade secrets and other confidential data, as well as to e-discovery. When employees store company data on their devices, that could invalidate the trade secrets, as they've left the employer's control. Given those email clients such as Outlook and Apple Mail store local copies (again, on smartphones, tablets, and home PCs) or server-based email, theoretically many companies' trade secrets are no longer secret.

A 2010 US Supreme Court 9-0 ruling declared that employees are not entitled to privacy if they use an employer’s issued device, so what level of privacy is there for BYODs? Will employees using BYODs be entitled to privacy if they are conducting business for their employers? Or will the employees using BYODs be entitled to privacy if the employer reimburses the employee for the cost(s) of the BYOD?

Wearable Devices Security Best Practices

For Wearable Devices content management include robust security and device management capabilities are the definition of best practices. CIOs and CSOs should implement the following:

Security Controls

- 256-bit AES encryption per file at rest, 30-day rotating encryption key - Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide.
- 256-bit SSL encrypted data transfer - 256-bit SSL Encryption provides an extra layer of protection for our users. This protection can help defend against login and password theft, which is particularly common in today's wireless society.

Remote Wearable Devices Management

- Automatic timed screen logout on devices that can display information
- At least a 4-digit passcode for each device
- Biometric security processes where possible like fingerprint or retina scanning for connectivity to the enterprise network
- Immediate access restriction on the device
- Automatic login to end-user accounts which includes the facility to remotely wipe all connection protocols, data, and software from the device
- Automatic shutdown and locking of a device after a security breach from a device
- Security breach reporting

Access Management Controls

- Prohibit access to Application / Web User Interface (UI) from the administrative console
- Prohibit access to content (folders and groups) from the administrative console
- Domain Identity Control: SSO - Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple software systems.

Wearable Device Applications

- Audit trail for discovery –monitored in real time by a dedicated security audit team or altering software
- All global files should be available to be accessed and managed (add, change, and delete) directly from the central restricted console -- This includes reporting on the access and use of these files by the device including IP addresses and login ids
- Reporting of all mobile device activity based on:
    - Usage statistics are tracked for files, individual users, and groups
    - Downloads, uploads, previews
    - IP Address

Legal Considerations

Privacy

One of the primary privacy considerations in a wearable device policy is the Stored Communications Act (SCA) which was enacted as part of the Electronic Communications Privacy Act (ECPA). The Stored Communications Act is outdated as its authors never contemplated the prevalence of social media and the Wearable Devices' computing environment.

The SCA deals with the voluntary and compelled disclosure of “stored wire and electronic communications and transactional records” retained by third-party internet service providers (ISPs). Also, it prohibits ISPs from divulging the contents of electronic communications carried, stored, or maintained by the service.

The Stored Communications Act (SCA) makes it an offense for a person or entity to intentionally access without authorization a facility that provides electronic communications service. It is also illegal to intentionally exceed authorization to access such a facility. The person or entity that obtains alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage can be fined or imprisoned. The person whose site has been violated can also seek a civil remedy for the offense.

The risk to employers who obtain unauthorized access to an employee’s private site first gained attention in 2009 with the *Pietryllo v. Hillstone Restaurant Group, d/b/a Houston’s case*. The company’s managers violated the SCA when they did not have authority from the site owners (the employees) to enter the site. The court also found that the managers invaded the privacy of the employees.

An SCA offense may also apply to unauthorized access to a member’s private site or group. So the message for every company is not to try to gain unauthorized access to an employee’s or member’s private site(s) or group(s). Also, do not ask an employee to provide you with the login codes or passwords to access any private sites. Even if the employee provides the information freely as in the *Pietryllo v. Hillstone* case, the employer has to show that the employee was not coerced or threatened to comply with your request.

Companies don’t have to stop monitoring because of the Stored Communications Act; they just have to be smart about it. If you ask the owner or administrator for access to a private site and they say no, walk away. Recognize the limitations imposed by employment and privacy laws on your ability to monitor employee sites.

Record Retention

Record Retention of Federal and State Requirements

Under Federal Rule 26(b)(2)(B), parties need not provide discovery of electronically stored information from sources that are not reasonably accessible because of undue burden or cost, unless the discovering party establishes good cause for the need for such information. The party asserting undue burden or cost must still identify the sources of information that are not reasonably accessible. Even if a party is excused from searching for and producing records that would be burdensome to produce, the party is not necessarily excused from its obligation to preserve such evidence, discussed below. It should be noted that even if production is unduly burdensome or costly, the court may still require production if the requesting party establishes a good cause.

The courts look to the reasonableness of a document retention policy. If the policy serves the legitimate business interests of an enterprise, complies with applicable statutory and regulatory requirements, is uniformly applied, and serves to preserve records that may be relevant to a claim or defense involved in threatened or pending litigation, there is little risk of court-imposed sanctions. By following the common-sense measures recommended the organization reduces its risk of legal sanctions and will be able to promptly and properly respond to discovery in the event of litigation or non-compliance during an audit.

Implications Sarbanes-Oxley and Gramm-Leach-Bliley

A business record is essentially any material that contains information about your company's plans, results, policies, or performance. In other words, anything about your company that can be represented with words or numbers can be considered a business record – and you are now expected to retain and manage every one of those records, for several years or even permanently depending on the nature of the information. The need to manage potentially millions of records each year creates many new challenges for your business, especially for your IT managers who must come up with rock-solid solutions to securely store and manage all this data.

Section 802 makes it a crime for anyone to intentionally destroy, alter, mutilate, conceal cover, or falsify any records documents, or tangible objects that are involved in or could be involved in, a US government investigation or prosecution of any matter, or in a Chapter 11 bankruptcy filing. Section 802 underscores the importance of record retention and destruction policies that affect all of a company's Email, Email attachments, and documents retained on computers – e-data – as well as hard copies of all company records.

The rules state that if you know your company is under investigation, or even suspect that it might be, all document destruction and alteration must stop immediately. And, you must create company records showing that you've ordered a halt to all automatic e-data destruction practices. Institutions also need to consider all other regulatory rules governing records retention within their industry. For example, for FFIEC, SEC, IRS, etc…most documents must be retained for 7 years.

Security Requirements

Minimum-security requirements for all information and data that affect the financial reporting of ENTERPRISE include at least the following.

- ***Data Security*** – Have a defined set of business and technical rules that clearly state what is expected with data that is captured and used by ENTERPRISE, customers, vendors, and all potentially interested outside parties.
- ***Organizational Security*** – Have a defined set of security guidelines within ENTERPRISE and ENTERPRISE's data that is accessed or processed externally.
- ***Asset Inventory*** – Have an inventory of all assets and established levels of security controls and protection commensurate with the impact of the assets on the books and records of ENTERPRISE.
- ***Procedural Standards*** – Document and communicate the procedures that must be followed daily, weekly, monthly, accounting period, and annually. Included are the processes to monitor the compliance and enforcement of the procedures.
- ***Physical and Environmental Security*** – Have a clear definition of the areas and access points to all assets and data that impact any of the items that are recorded in the "books and records" of ENTERPRISE.
- ***Operations and Communication Security*** – Have processes in place to ensure the security of the dissemination of information, including retrieval, input, modification, backup, and destruction through networks, software, hardware, and physical copies.
- ***Access Control*** – Have a process in place a process for controlling physical and electronic access. This includes protecting all access to the system by unauthorized individuals internal and external to ENTERPRISE.
- ***System Development, Operation, and Maintenance*** – Have processes in place that ensure the system of internal controls is in place, including checks and balances that will negate the possibility of "back doors" and other unauthorized access to ENTERPRISE's assets, information, systems, and data.
- ***Business Continuity and Disaster Recovery*** – Have processes in place to ensure the survivability of the ENTERPRISE in face of major disruptions of its operations (see https://ww.e-janco.com/drp.htm).
- ***Compliance*** – Have processes in place to validate compliance with the Security Standard including auditing, monitoring, and maintenance of the standards. These processes should include methods for prevention, detection, and correction of defects to the compliance processes.

WYOD Management Security Options

As more WYOD devices can access confidential and proprietary information, companies need to consider the options they have to secure their assets (data) on these devices for when employees are terminated, devices are lost, or stolen.

The options to consider are:

- Remote Lockout
- Remote Wipe 100% or the selective wipeout of company applications and data
- Over-the-air management of the device
- On-Device encryption
- Over-the-air data encryption
- Complex passwords
- Two-factor authentication
- Biometrics for access
- Automatically enforced password policies
- VPN only access
- Video and sound disable
- Restrict and/or block application store
- Restrict and/or block wireless LANs
- Automatic enforcement and management of policies

Appendix

Top 10 WYOD Best Practices

Employees bringing their smartphones into the workplace started the BYOD trend requiring enterprises to deal with the serious security implications that come from these devices. The decision for employees to wear their device (WYOD), such as an apple watch that can link to your WiFi; capture audio, video, and data; store; and transmit poses similar problems for IT departments. Employees and individuals outside of the enterprise can use these devices, sometimes discretely, to access and share business content.

This puts corporate data and infrastructure at risk and reinforces the need for IT managers to focus on securing the content, rather than the device that's in use. Wearable devices simply add another level of access and security concern to what we've already seen with the BYOD trend.

Here are the top 10 best practices for WYOD.

1. **Have a strategy for how, when, and why WYOD devices can be used**. This should include both internal operations and external ones that are available to the general public.
2. **Implement an acceptable use policy**. Include legal references and methods of communication of that policy to those outside of the organization.
3. **Identify the connectivity options that are available to both internal and external users**. Include security and compliance in the creation of the options available.
4. **Approved devices should be easily connected to the available secure access points**. There should have to be minimal involvement from IT staff.
5. **Define a management process for the WYOD devices**. Consumer devices are designed to be managed by an individual, not in mass, and although these endpoints may be outside of the control of IT they need to be managed because they represent a tremendous productivity tool as well as a very advanced piece of technology. It's important to keep in mind that these devices are often as powerful and capable as an employee's laptop or PC, but instead of physically residing inside the corporate walls, they are often sitting on the table at a coffee house or beside a pool at a hotel.
6. **Plan for the activity WYOD devices will add to the network**. Consumer devices are voice, video, high-definition image, and application-rich. Employees using these devices will devour bandwidth and network resources. Assess your existing switch and router networks, your wired and wireless access in-branch and home offices, the size of your internet pipes, and connections to remote locations. Make adjustments in advance of the increased demands that are inevitable on your IT network infrastructure grid.
7. **Make collaboration tools a priority**. Although consumer devices offer social and digital options natively, don't be content with just consumer-grade capabilities, extend your organization's collaboration tools for enterprise mobility, integrated voice, video, messaging, conferencing, application sharing, presence, and single number reach to realize even greater productivity gains.
8. **Secure the endpoints and isolate sensitive/confidential information and locations**. What is your strategy, especially important in highly regulated industries such as healthcare and finance that require strict security and compliance controls? Review WiFi security, VPN access, and perhaps add-on software to protect against malware. Consider two-factor authentication technologies.
9. **Be prepared for little to no advance notice of upgrades**. Third parties like Apple and Samsung are not part of your company's Change Management Process. Expect new code to be dropped on your corporate endpoints overnight creating connectivity, application, and security issues.
10. **Formalize your 7 x 24 support**. If employees are going to work in the evening, on weekends, or take time away from a family vacation, IT systems must be available when they do. Downtime is no longer an option. Either bring in tools and staff around the clock or engage an IT-managed service organization to provide the coverage you need.

Electronic Forms

Three (3) Electronic form is included with this policy template. It comes separately in its directory.

Mobile Device Access and Use Agreement

Mobile Device Security and Compliance Checklist

Wearable Device Access and Use Agreement

What's New

2023 Edition

- Update to meet the latest mandated requirements and ISO compliance standards
- Updated all included forms

2022 Edition

- Update to meet the latest mandated requirements and ISO compliance standards
- Updated all included forms

2021 Edition

- Added two electronic forms
  - Mobile Device Access and Use Agreement
  - Mobile Device Security and Compliance Checklist
- Updated all included forms
- Added section on device and data ownership – focus on WFH

2020 Edition

- Updated to meet GDPR and CCPA-mandated requirements
- Updated included electronic form

Work From Home & Telecommuting Policy

2023 Edition

License Conditions

Published by: **Janco Associates Inc.**
Park City, UT 84060

435 940-9300 -- Email – **support@e-janco.com**

Table of Contents

_Toc100658612

Work From Home (WFH) & Telecommuting Policy

Overview

This policy permits ENTERPRISE to designate employees to work at alternate work locations for all or part of their workweek to promote general work efficiencies or to meet particular work requirements of individual employees and/or departments of ENTERPRISE.

ENTERPRISE managers are responsible for managing the affairs and operations of ENTERPRISE; thus, managers authorized to set working arrangements (locations and hours), under this policy have the discretion to:

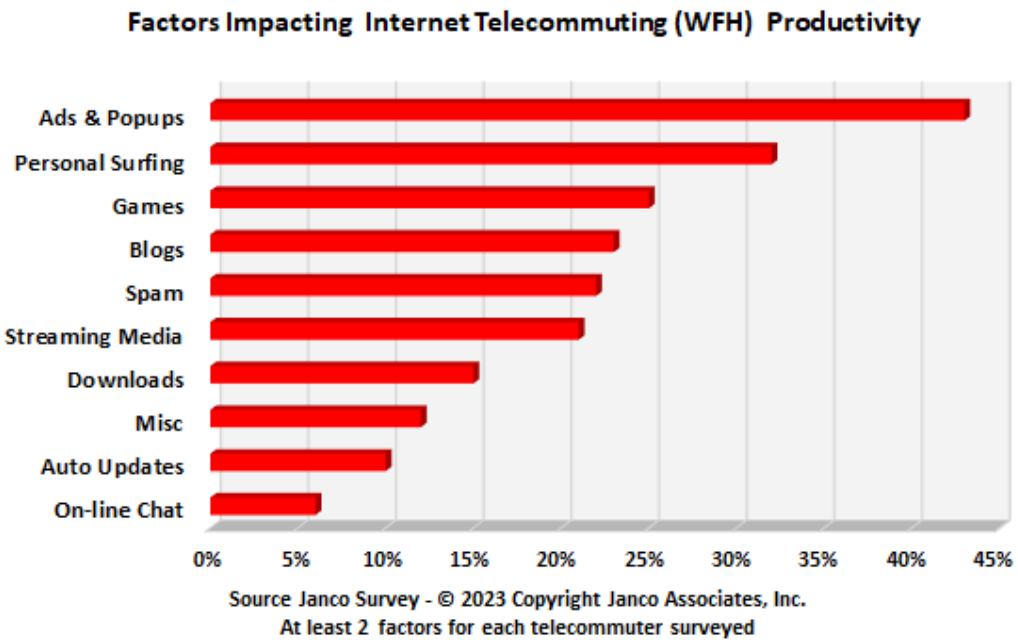
- Designate positions eligible for WFH and telecommuting; and
- Approve employees to WFH and telecommute.

WFH and telecommuting assignments do not change the conditions of employment or required compliance with other ENTERPRISE policies. Managers with the approval of Human Resources may establish WFH and telecommuting as a condition of employment. In such cases, this requirement should be included when the position is advertised and in correspondence offering employment.

Telecommuting resource misuse can have serious implications for an enterprise

When workers telecommute, many factors can impact their overall effectiveness and thusly increase costs and risks to the company.

- **Reduced productivity** - If employees spend their time on social networking sites such as Facebook, they're not spending it doing their job.
- **Security risks** - Malware hides on websites and can install itself as users browse infected pages. It has been reported that the number of new, malicious websites blocked each day nearly doubled.
- **Legal risks** - When users download inappropriate material to their computers other employees may take serious offense which in turn can create legal liabilities for managers.
- **Wasted bandwidth** - Internet connections cost money. If half your bandwidth is taken up with non-work-related web traffic, you could potentially be paying twice as much as you need to and your business-critical communications could be running at half their speed capacity.
- **Unlicensed software** - When users download and install software from the internet, they create legal risks. Software piracy is illegal. If an organization uses illegal copies of the software, it may face a civil suit and company directors risk criminal penalties.
- **Reputation risk** - Social networking can create opportunities for employees to leak confidential information or spread damaging rumors online. Bad behavior by a single employee can reflect on the reputation of the whole organization.



Policy

To foster employee and ENTERPRISE efficiencies, it is the policy of ENTERPRISE to allow employees to WFH and/or telecommute. Telecommuting is a work arrangement in which some or all of the work is performed at a worksite such as the home or in an office space near home or a travel location such as a hotel or an airport business center.

Communication may be by one of several means, such as phone, modem, fax, and pager. Equipment may be owned and maintained by the employee or by ENTERPRISE.

Managers must follow the guidelines within this policy and have approval from the Human Resources Department to implement this policy.

Policy Definitions

The following are definitions that apply to this policy:

- **Alternate Work Location** - Approved worksites other than the employee's central workplace where ENTERPRISE business is performed. Such locations may include but are not necessarily limited to, employees' homes, satellite offices, hotels, or airport business centers.
- **Central Workplace** - An employer's place of work where employees normally are located.
- **Employee** - An employee who works away from his/her central workplace either at home or another ENTERPRISE-designated or approved remote work location.
- **Telecommuting** - A work arrangement in which supervisors direct or permit employees to perform their usual job duties away from their central workplace, per work agreements.
- **Work Agreement** - The written agreement between ENTERPRISE and the employee that details the terms and conditions of an employee's work away from his or her central workplace. Work agreements are required for Telecommuting.
- **Work Schedule** - The employee's hours of work in the central workplace or alternate work locations.

ENTERPRISE Responsibilities

Work performed in alternate work locations is considered ENTERPRISE business; therefore, ENTERPRISE establishes specific conditions that apply to employees working in alternate locations.

ENTERPRISE Policy Requirements

ENTERPRISE has established internal policies and procedures related to all work locations and these must be followed. These policies maximize the appropriate use of telecommuting without diminishing employee performance or service delivery. ENTERPRISE will:

- Identify positions that are appropriate for WFH and telecommuting.
- Requires work agreements between ENTERPRISE and employees.
- Require compliance with local zoning regulations and mandated requirements.

Termination of Agreement

ENTERPRISE may terminate the WFH and telecommuting agreement at its discretion. ENTERPRISE will give typically employees one (1) week advance notice if a decision is made to terminate a WFH and/or telecommuting agreement; however, advance notice is not required.

Terms and Conditions

Compensation and Benefits

An employee's compensation and benefits will not change because of WFH or telecommuting. Any additional expenses the employee incurs can be reimbursed if there is prior written approval by the employee's direct supervisor or manager.

Hourly employees are NOT authorized to work more than 8 hours per day and 40 hours per week without written approval. Any time worked beyond that is at the employee's discretion and will not be compensated.

Hours of Work

The total number of hours that employees are expected to work will not change, regardless of work location. Employees agree to apply themselves to their work during work hours.

ENTERPRISE must ensure that procedures are in place to document the work hours of employees who WFH and/or telecommute, ensuring compliance with the Fair Labor Standards Act.

Telecommuting is not intended to serve as a substitute for child or adult care. If children or adults in need of primary care are in the alternate work location during employees' work hours, some other individuals must be present to provide the care.

Attendance at Meetings

Supervisors may require employees to report to a central workplace as needed for work-related meetings or other events or may meet with the employee in the alternate work location as needed to discuss work progress or other work-related issues.

If possible, employees can attend these meetings via teleconferencing if those facilities are available.

Sick Leave and Time Off

Telecommuting is not intended to be used in place of sick leave, family and medical leave, leave used under the State and Federal sickness and disability Programs, workers' compensation leave, or other types of leave.

However, ENTERPRISE may determine whether or not it is appropriate to offer to telecommute as an opportunity for a partial or full return to work based on ENTERPRISE policy and the criteria normally applied to decisions regarding the approval of telecommuting.

Workers' Compensation and Safety Program Liability

ENTERPRISE may be liable for job-related injuries or illnesses that occur during employees' established work hours in their alternate work locations. It is, for this reason, ENTERPRISE has the right to inspect the alternative work location and see that it complies with all mandated requirements and meets ENTERPRISE's Safety Program requirements.

Equipment and Supplies

Normally, ENTERPRISE will provide the equipment and supplies needed by employees to effectively perform their duties. However, where agreements specify, employees may be authorized to use their personal equipment. In all cases, all data and sensitive information will remain the property of ENTERPRISE.

The employees will comply with all backup, record retention, security, sensitive information, business continuity policies, and procedures of ENTERPRISE.

Under no condition shall any individual (especially children) utilize any computer, USB storage device, PDA, Smartphone, or another device that contains ENTERPRISE data.

Enterprise Owed Equipment

- Authorized use/users – ENTERPRISE-owned equipment may be used only for legitimate business purposes by authorized employees.
- Employees are responsible for protecting ENTERPRISE-owned equipment from theft, damage, and unauthorized use.
- Maintenance – ENTERPRISE-owned equipment used in the normal course of employment will be maintained, serviced, and repaired by ENTERPRISE.
- Transporting/Installing – ENTERPRISE Information Technology employees are responsible for transporting and installing equipment, and for returning it to the central workplace for repairs or service. When this occurs IT employees shall have the right to inspect the location where the equipment is located to see that the location complies with all ENTERPRISE policies.

Employee-Owned Equipment

- When employees are authorized to use their personal equipment, ENTERPRISE does not assume responsibility for the cost of equipment, repair, or service.

Record Management Process and BCP

Records that are created and received by the telecommuter need to comply with the company's records management, retention, and destruction policy. Also, processes need to be in place which will be considered, and in Business Continuity and Disaster Recovery plans. The telecommuter needs to be versed in these plans and comply with all the necessary procedures associated with them.

BYOD Security

By adopting strategies that are flexible and scalable and taking advantage of new and upcoming security features, ENTERPRISE will be better equipped to deal with incoming challenges to their security infrastructure posed using employees' own devices.

- Follow the formal BYOD policies of ENTERPRISE.
- Implement locking of the device after 5 minutes of inactivity.
- Implement a remote wipe of the BYOD if the device is lost or stolen.
- Limit the storage of sensitive and confidential information.

Telecommuting costs

ENTERPRISE does not assume responsibility for operating costs, home maintenance, or other costs incurred by employees in the use of their homes as telecommuting alternate work locations, except:

- Pay for leased telephone lines and/or broadband connectivity in the employee's alternate work location,
- Install, and provide basic telephone service and/or broadband connectivity in employees' alternate work locations or
- Provide cell phones to employees for business use.
- If cell phones are not provided, ENTERPRISE may reimburse employees for business-related long-distance calls made from their personal telephones.
- Office supplies such as stationery, toner/ink cartridges, blank DVD/CDROMs for backup, and other normal supplies.
- Licensed software remains the property of ENTERPRISE.

Work Agreements

ENTERPRISE and employees must agree to the terms of WFH and/or telecommuting before an employee may work at an alternate work location.

ENTERPRISE agreements must be reviewed and approved by the Human Resources and Legal Departments before use.

- Duration of the agreement;
- Work schedule and how it can be changed;
- How time off is requested and approved by the supervisors;
- Status of employees during an emergency or weather-related closing affecting the central or alternate workplace;
- How routine communication between the employee, supervisor, co-employees, and customers will be handled;
- Employee's performance plan/expectations;
- Equipment and/or supplies that will be used, and who is responsible for providing and maintaining them;
- Applicable data security procedures;
- Safety requirements; and
- Employees permit supervisors or anyone authorized by them to access the alternate work location during normal work hours as defined by the telecommuting agreement.
- Comply with all ENTERPRISE, local, state, and federal rules, policies, practices, and instructions;
- Use ENTERPRISE-provided equipment/supplies only for business purposes, and to notify ENTERPRISE immediately when equipment malfunctions;

- Notify their supervisors immediately of any situations which interfere with their ability to perform their jobs;
- Maintain safe work conditions and practice appropriate safety habits;
- Certify that the work location is free from hazards;
- Notify their supervisors immediately of any injury incurring while working;
- Agree to allow supervisors to visit the alternate work location immediately after an accident or injury that occurred while working;
- Absolve ENTERPRISE from liability for damages to real or personal property resulting from participation in the telecommuting program; and
- Be responsible for the security of information, documents, and records in their possession or used during telecommuting, and do not take restricted-access material home without the written consent of their supervisors.

BYOD, Tablets, PDAs, and Smartphones

Regardless of whether telecommuters work on their own (BYOD) tablets, PDAs, or Smartphones or are corporate-issued ones, the policy of ENTERPRISE is that these users must follow IT to support the management, tracking, securing, and supporting of these devices, just like they do for any other corporate computing platform.

Specifically, the policies that apply to these types of devices are:

- Comply with security best practices for tablets, including the use of multilevel passwords and device certificates, and the ability to remotely wipe the device if it is lost or stolen.
- Utilize tiered access to network resources to secure critical data and applications.
- Comply with application delivery mechanisms.

Work From Home

The Work From Home (WFH) environment is different than telecommuting in that the individuals are primarily out of the office almost all of the time. In contrast to traditional telecommuters who are out of the office some of the time and/or choose to work during off-hours or when they are traveling.

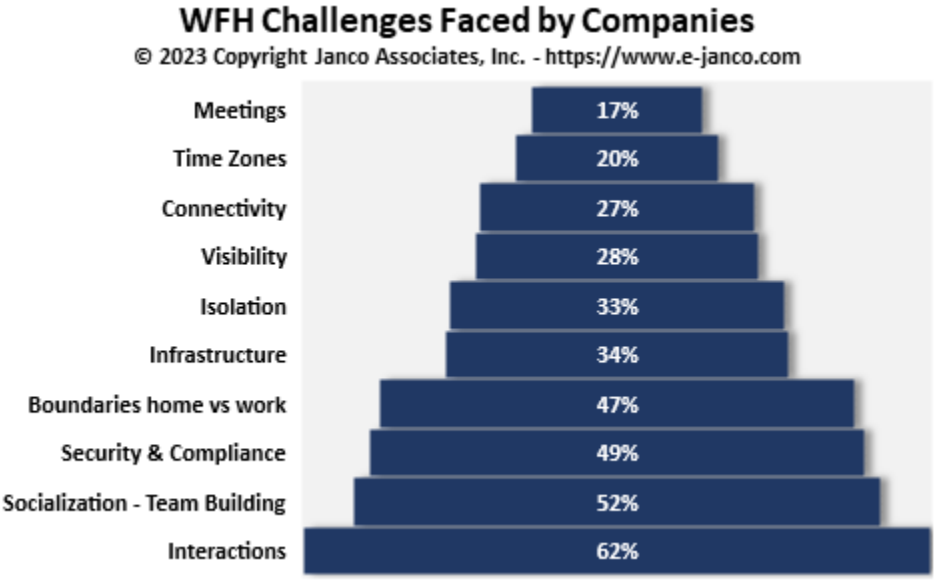
WFH Operational Rules

The WFH environment, from an external view, should be as close to the in-office environment. Rules need to be in place to support that. That includes following all of the security, record management, and compliance requirements that are utilized for the in-office environment.

- Record management policies need to be complied with.
- DR/BC process should be in place for WFH locations.
- Security and safety policies need to be integrated into the WFH environment
    - VPN should be used when accessing any confidential, proprietary, or sensitive information
    - Virus protection should be implemented on all devices accessing any confidential, proprietary, or sensitive information
    - Malware protection should be implemented on all devices accessing any confidential, proprietary, or sensitive information including browsers and email accounts
- Office hours for the WFH workers should be the same as when they are in the office. The worker needs to be available during those hours.
- Voice Mail needs to be followed up promptly – Voice mail is not defined or full it is not acceptable.
- E-Mail accounts need to be monitored and e-Mails addressed promptly.

WFH Challenges Faced

In a survey of over one hundred plus companies, Janco has identified the top 10 challenges faced by companies. These challenges and others have to be considered given the operational environment of the enterprise.



Interactions

When WFH is in place at an enterprise, one of the major challenges is the interaction between staff and management, suppliers and customers, and other individuals key to the enterprise's mission. For example, since staff and management are not at the same location, the process of a "quick" question and or idea is not as easily facilitated. Processes need to be put in place which will foster the ideas of communication without the inefficiencies of interruptions.

Socialization- Team building

In the in-office environment staff and management interact constantly during the workday. Breaks, lunches, and after-hours get-togethers all are part of the team-building process. These avenues are not available for WFH workers.

Security and Compliance

WFH exposes digital assets both at the WFH location and on BYOD devices. Digital assets and printed documents at the WFH location need to be protected from inadvertent exposure. Also, mandated compliance requirements for security and records management policies can be difficult to monitor.

Boundaries – Home vs Work

Few individuals have had the experience of working at home. Challenges arise with the worker and other individuals in the house. What is a person to do when a child or pet invades the workspace of the worker during a critical phone call or electronic meeting? The at-home work environment needs to be set up in such a way the worker is viewed as not at home but in the office. That is a challenge, to say the least.

Infrastructure

Stresses are placed on the enterprise's overall operational performance. Everything from IT infrastructure to following up with customers and sales and distribution may not be adapted to the WFH environment.

Isolation

When people are in the WFH environment they become isolated from the rest of the company in addition to other people. This causes stress and can lead to an environment in with they do not function in the same way as when they are in the office.

Visibility

Is WFH working, who are the top performers, and who is not meeting the enterprise's performance and operational objectives? These are questions that need to be answered.

Communication

WFH locations' connectivity with the internet is location and equipment dependent. Not every WFH location may have the necessary "broadband" service that is needed to support the WFH worker. Also, technical support may need to be dispatched to support the WFH worker as the workers may not have the necessary expertise to resolve issues as they occur.

Time Zones

WFH employees may choose to operate from a location other than one that is in the same time zone. The hours of operation should be well understood, and calendars should be synchronized to the office hour time zone.

Meetings

Electronic meetings for WFH workers present unique requirements from dress code to the background of participants.

Appendix

Employer Legal Workplace Responsibilities

The legal responsibilities of the employer in the workplace apply equally to the home working and all other "out of office" environments. Legislation applicable includes various regulations in the United States, US, EU, and other jurisdictions:

- **Americans with Disabilities Act Amendments Act (2008)**: The ADA does not require an employer to offer a telework program to all employees. However, if an employer does offer telework, it must allow employees with disabilities an equal opportunity to participate in such a program. Changing the location where work is performed may fall under the ADA's reasonable accommodation requirement of modifying workplace policies, even if the employer does not allow other employees to telework. However, an employer is not obligated to adopt an employee's preferred or requested accommodation and may instead offer alternate accommodations if they would be effective.
- **Occupational Safety and Health Act** is the primary US law that governs occupational health and safety in the private sector and the federal government in the United States. In essence, the company needs to have a Safety Program in place that covers out-of-office locations.
- **Data Protection Act (1998)**: concerns the processing and storage of personal information, irrespective of where this is carried out. Is the data secured against theft and viewing by family members and visitors?
- **Health and Safety at Work Act (1974)**: ensure the welfare, health, and safety of employees wherever they work. Under section 2(4) of the Act safety representatives, appointed by a recognized Trade Union, can represent home workers in any consultations with employers concerning health and safety, and welfare matters.
- **Working Time Regulations (1998)**: stipulate that, unless opted out of, workers should work no more than 48 hours per week. They also provide directives on breaks taken and paid annual leave.
- **Display Screen Equipment Regulations (1992) (amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002)**: anyone, including remote workers, who use computers regularly (i.e. for a third or more of their working time for a continuous period of one month), is entitled to an eye test paid for by their employer.
- **Reporting of Injuries, Diseases, and Dangerous Occurrences Regulations (RIDDOR) 1995**: employers must report and record work-related accidents, injuries, and other occurrences arising from work-related activities, including home working.
- **Employment Act (2002)**: an employer may reject any application to commence remote work if the desired working pattern cannot be accommodated by the needs of the business.

Position Requirements for Qualification for WFH & Telecommuting

Determining positions that are appropriate for WFH & telecommuting

In making decisions about which positions are appropriate to designate or approve for telecommuting, Managers should thoroughly analyze the duties of positions and how their work is performed. Included in this analysis are:

- Require independent work.
- Require little face-to-face interaction.
- Require concentration.
- Result in specific, measurable work products.
- Can be monitored by output, not time spent doing the job.

Employee qualities that are appropriate for WFH & telecommuting

In making decisions about which employees are designated or approved for telecommuting, managers should review the work qualities of employees, in addition to ensuring that their positions are appropriate for telecommuting. Included in this analysis are:

- Can work productively on their own.
- Are self-motivated and flexible.
- Are knowledgeable about the job.
- Have a low need for social interaction.
- Are dependable and trustworthy.
- Have above-average performance records.
- Are organized.
- Have good communication skills.

Top 10 Best Practices

- Have a plan for the work and schedule for each telecommuting employee.
- Have every employee report to their manager, with a brief email that lists his or her achievements, upcoming goals, and any obstacles that may be in the way.
- Have managers focus on removing obstacles and keeping people productive.
- Have managers create KPI metrics. Capture and communicate status up and down the organization.
- Validate that managers have at least weekly, if not daily, video conferences with their team.
- Build team morale and keep people focused on business goals.
- Monitor security and compliance on an ongoing basis
- Have the IT help desk provide tips to the employees on how to manage their Internet connections. For example, ask others on the same Internet connection to pause non-business-related internet activity while video conferencing with others.
- Management team members should engage the teams in discussions about how they can improve productivity. (i.e., What can the team do to improve customer satisfaction, the supply chain, order processing, etc.?)
- C-Level executives should work with their leadership teams and the Board of Directors to start shaping a new strategy. There is time to adjust or redefine, enterprise strategy to operate more effectively in a WFH & telecommuting environment.

Job Description

Full job descriptions are included with this policy template. They come separately in their directory.

Manager Telecommuting

Manager Work From Home Support

Electronic Forms

Electronic forms are included with this policy template. They come separately in their directory.

Enterprise Owned Equipment

Internet and Electronic Communication Agreement

Mobile Device Access and Use Agreement

Mobile Device Security and Compliance Checklist

Privacy Policy Compliance Agreement

Remote Location Contact Information

Safety Checklist - Work at Alternative Location

Security Access Application Mobile

Sensitive Information Policy Compliance Agreement

Social Networking Policy Compliance Agreement

Telecommuting IT Checklist

Telecommuting Work Agreement

Text Messaging Sensitive Information Agreement

Work From Home Contact Administration

Work From Home IT Checklist

Work From Home Work Agreement

What's New

2023 Edition

- Updated all survey data with the most recent results
- Updated all the Electronic Forms
- Updated all included job descriptions

2022 Edition

- Added top 10 best practices for WFH and telecommuting users
- Updated all survey data with the most recent results
- Updated all the Electronic Forms
- Updated all included job descriptions

2021 Edition

- Expanded for Work From Home
- Added section on Work From Home Best Practices
- Added a job description for Manager WFH Support
- Updated all the Electronic Forms
- Updated all included job descriptions
- Added three (3) Work From Home forms
  - Work From Home Contact Information
  - Work From Home IT Checklist
  - Work From Home Work Agreement

2020 Edition

- Added a Job Description for Manager Telecommuting
- Add five (5) electronic forms
  - Privacy Policy Compliance Agreement
  - Remote Location Contact Information
  - Sensitive Information Policy Compliance Agreement
  - Social Networking Policy Compliance Agreement
  - Text Messaging Sensitive Information Agreement
- Updated all of the electronic forms

JANCO ASSOCIATES, INC.

BYOD Support Specialist

Position Purpose

The BYOD Support Specialist is responsible for the overall coordination, control, and maintenance of all BYODs within the enterprise to ensure compatibility and integration with enterprise strategies.

Problems and Challenges

Mobile computing is an emerging technology that is evolving dynamically and requires constant review and evaluation to ensure that planning and budgeting activities position the enterprise to take full advantage of applicable advancements. The specialist is challenged to establish a level of credibility within the personal mobile computing function that will entice clients to consult with that function as opposed to individual evaluation. This will ensure compatibility with enterprise strategies and maximize returns on investments.

Essential Position Functions

Principal Accountabilities

- Identifies and initiates resolutions to client problems and concerns associated with personal mobile computing equipment, hardware, and software to the client's satisfaction.
- Works closely with the help desk function to ensure that a knowledge base of mobile computing issues is documented, accurate, and current.
- Plans and coordinates the purchase, installation, and implementation of personal mobile computing hardware and software according to department standards and procedures.
- Analyzes training needs of personal mobile computing clients
- Develops classroom curriculum and provides quality individual and group training programs designed to ensure maximum utilization of equipment.
- Ensures that the security standards of the enterprise are maintained.
- Maintains anti-virus software updates.
- Monitors compliance of users to the enterprise's security and records management policies by the users with personal mobile devices.
- Maintains registration logs and inventory to provide upgrades as necessary and ensure appropriate security levels are maintained.
- Upholds the enterprise policy guidelines as well as recommends new and improved guidelines to ensure compatibility and better service enterprise users of personal mobile devices.
- Maintains current technical expertise in the rapidly changing technology and utilizes state-of-the-art techniques when implementing personal mobile computing solutions.
- Prepares weekly status reports quantitatively reporting results of personal mobile computing activities.

- Maintains a positive working relationship with all enterprise departments to optimize working relationships and communication.
- Fulfills department requirements in terms of providing work coverage and administrative notification during periods of personal illness, vacation, or education.
- Performs at or above enterprise performance standards established within the department.

Authority

- Resolve problems with client mobile computing hardware and software.
- Plan and coordinate mobile computing hardware and software purchases and implementations.
- Analyze training needs and develop training programs and curricula.

Contacts

The BYOD Support Specialist works with mobile computing users within the enterprise as well as with external vendors.

Position Requirements

- A high school diploma or equivalent is required
- BS or BA degree in computer science, business administration, or a related field is preferred
- 3 years of personal computer experience
- 2 years of experience in a training environment
- Strong written and verbal communication skills

Career Ladder

The career track for this position is continual technical leadership within operations, technical services, and user organizations.

BYOD Support Supervisor

Position Purpose

The BYOD Support Supervisor is responsible for the overall coordination, control, and maintenance of BYOD devices within the enterprise to ensure compatibility and integration with enterprise strategies. The supervisor reports to the Manager Microcomputer Technology.

Problems and Challenges

The BYOD Support Supervisor is challenged with establishing and maintaining a high level of creditability for the function, enticing clients to consult with the function ensuring compatibility with enterprise strategies, and maximizing returns on investments. In meeting these challenges the BYOD Support Supervisor must constantly review, evaluate, plan, and budget activities in this dramatically and constantly evolving technological arena.

Essential Position Functions

Principal Accountabilities

- Identifies and initiates resolutions to user problems and concerns associated with BYOD devices, hardware, and software to the user's satisfaction.
- Plans and coordinates the purchase, installation, and implementation of BYOD hardware and software according to department standards and procedures.
- Analyzes the training needs of personal computer users,
- Develops classroom curriculum and provides quality individual and group training programs designed to ensure maximum utilization of BYOD equipment.
- Maintains BYOD software and hardware registration and inventory to provide upgrades as necessary and ensure appropriate security levels are maintained.
- Upholds the enterprise policy guidelines as well as recommends new and improved guidelines to ensure compatibility and better service to BYOD users.
- Maintains current technical expertise in the rapidly changing technology of BYOD devices.
- Utilizes state-of-the-art techniques when implementing hardware and software solutions.
- Prepares monthly status reports quantitatively reporting results of BYOD activities.
- Adheres to and maintains a positive working relationship with all enterprise departments to optimize working relationships and communication.
- Fulfills department requirements in terms of providing work coverage and administrative notification during periods of personal illness, vacation, or education.
- Performs at or above the enterprise's Information Technology performance standard.

Authority

- Resolve problems directly with client BYOD hardware and software.
- Plan and coordinate BYOD hardware and software purchase and implementation.
- Develop PC training programs and curricula commensurate with needs.
- Work with BYOD users within the enterprise and with BYOD vendors.

Contacts

Routine contact is required with IT application development and support personnel. Within the business, routine contact is required with end-user personnel.

Position Requirements

- BS or BA in business administration or computer science is desired
- 3 years of personal computer experience
- 2 years of experience in a training or support environment
- Strong written and verbal communication skills

Career Ladder

This position will lead to increased responsibilities in the microcomputer technology area. A specific managerial position above this one would be Manager BYOD Support.

BYOD Support Supervisor

Chief Experience Officer (CXO)

Position Purpose

The Chief Experience Officer (CXO) is the executive responsible for the overall experience of customers, suppliers, partners, associates, and internal staff with an organization's products and services. The individual drives the enterprise's growth in the user experience arena. They oversee operations in all user experience sectors like marketing, image setting, mobile applications, social media, related technologies, virtual goods, as well as web-based management and marketing.

The CXO is not only a user experience expert but also seasoned marketing, brand, and product manager. As the role is transformational, the CXOs is responsible for the adoption of consistent user interfaces across the entire business. As with most senior executive titles, the responsibilities are set by the organization's board of directors or other authority, depending on the organization's legal structure.

Problems and Challenges

The major challenge for the Chief Experience Officer (CXO) is developing all revenue and profit-generating experiences offered to customers. This accomplished by is defining the user experience architecture while balancing user experience assets and computing services with financial and marketing needs. Seamless integration of user experience assets from the customer, through product and service design, and through management, reporting is a primary concern.

The overall user experience is the focal point for the CXO. The CXO's continued role is to assure the success of these areas while simultaneously minimizing costs and operational efficiencies.

Challenges include:

- Sparking energy, excitement, and action among people throughout the company.
- Taking the raw material of company capabilities and working with the organization to shape them into experience offerings.
- Aligning the various elements of operations to fit into a cohesive whole through a customer-pleasing theme.
- Fighting for the needs, wants, and desires of customers and making sure that the company's offerings create value on behalf of each guest.
- Propelling the enterprises in transforming into becoming premier experience stagers with the ongoing ability to regenerate new and world-class offerings – which include the goods and services on which experiences are staged.

Essential Position Functions

The CXO principal accountabilities are centered around the main objectives of the role. The objectives are:

- Promote the culture of customer orientation internally
- Develop knowledge and understanding of customers
- Implement targeted campaigns to increase customer loyalty, retention, and satisfaction
- Promote the customer perspective and make sure it is considered for all topics and projects of the organization
- Measure all the factors that form the customer experience through various KPIs.

Principal Accountabilities

- Ensures all user experience content is on-brand, consistent in terms of style, quality, and tone, and optimized for search and user experience for all channels of content including online, social media, email, point of purchase, mobile, video, print, and in-person.
- Maps out a strategy that supports and extends marketing initiatives, both short and long-term, determining which methods work.
- Develops a functional user experience content calendar throughout the enterprise verticals and define the owners within the enterprise.
- Supervises writers, editors, and content strategists; be an arbiter of best practices in grammar, messaging, writing, and style.
- Integrates all user experience activities within traditional marketing campaigns.
- Conducts ongoing usability tests to gauge user experience. Gathering data and handling analytics (or supervising those who do) and making recommendations based on those results.
- Works with owners of particular user experience points of contact to revise and measure particular content and marketing goals
- Creates, plans, implements, and monitors the user experience strategy for the company. Keeps the strategy fresh by staying up to date with the latest innovations, changes in competition, and shifts in the market.
- Charged with communicating the organization's user experience strategy and simplifying it over time so that it’s embedded in every operational application.
- Adapting the strategy over time to meet the movement of the market and the practicalities of execution.
- Obtains company-wide commitment to the user experience strategy.
- Connects with experts in the company and the broader industry and can adapt to the changes in the user experience strategy of the company
- Maintains focus on and commitment to executing the strategy for multiple years.

- Participates as a member of the senior management team in governance processes of the organization's, customer relationships, infrastructure architecture, telecommunications, networks, programming, media, and desktops.
- Leads strategic technological planning to achieve business goals by prioritizing user experience strategy initiatives and coordinating the evaluation, deployment, and management of current and future technologies.
- Collaborates with the appropriate departments to develop and maintain a user experience plan that supports organizational needs.
- Researches to remain up-to-date and knowledgeable about industry trends and emerging technologies in anticipation of new user experience processes and system alterations.
- Analyzes and improves upon user experience standards across the organization to maintain a technological and competitive edge within the market.
- Acts as the primary liaison for the company's user experience vision via regular written and in-person communications with the organization's executives, department heads, and end-users.
- Creatively and independently provides resolution to user experience problems in a cost-effective manner.
- Supervises recruitment, development, retention, and organization of all technical staff following corporate budgetary objectives and personnel policies.
- Ensures continuous delivery of user experience services through oversight of service level agreements with end users and monitoring of systems, programs, and equipment performance.
- Develops and communicates business/technology alignment plans to the executive team, staff, partners, customers, and stakeholders.
- Assists in the development and execution of enterprise-wide disaster recovery and business continuity plans.
- Provides a leadership role in the design and implementation of user experience strategy, including hardware, software, operating system software, and productivity tools.
- Develops plans for the migration of technologies to support necessary future directions.
- Develops long-range user experience architecture and strategy as it is applied to all phases of the enterprise's operations and interactions with its customers and suppliers.
- Provides enterprise-wide direction for the use of emerging user experience technologies for its satellite operations, including other groups and subsidiaries.
- Defines paths for a necessary capacity increase for all user experience technology within the enterprise including; product design, customer relationship management, and computer and communications hardware and software.
- Defines new approaches for user experience technology including hardware, software, productivity tools, databases, CASE tools, image processing, and multimedia.
- Defines enterprise user experience objectives and plans in the areas of technologies to facilitate its orderly and efficient implementation.
- Provides direction to all user experience assets within the enterprise to maintain the maximum efficiency of the enterprise's capital and human resources including hardware, software, and personnel.

- Defines user experience standards to ensure that all problems are solved in a timely and efficient manner including the contribution to the enterprise's enterprise contingency plan in the case of major interruptions in the product or service offerings of the enterprise.
- Defines standards for purchasing, identifying, evaluating, selecting, implementing, and managing the user experience strategy of the enterprise.
- Defines standards for training, equipment cost and usage, cost/usage ratios, usage procedures, and technical personnel time/project allocation.
- Defines the direction of in-house technical training seminars to improve overall employee awareness, response time, and the ability to investigate the future of the technological requirements of the enterprise.
- Defines standards and requirements for user experience products and services including all resources.
- Markets technology through the development of online newsletters and development of specific user groups.
- Defines which user experience technologies are recommended or required by the enterprise and its SBUs.
- Maintains current knowledge of user experience innovations and develops plans to utilize appropriate technologies in support of future enterprise business operations and expansions.
- Reviews cost estimates for personnel requirements, technology upgrades or additions, and external consulting projects in support of other departments and SBUs.
- Participates in local and national user group presentations, and publishes articles describing enterprise activities and assessments of technology and how it relates to the business.
- Interacts frequently with all SBU management on internal and external operations that are impacted by technology including review and approval of all major contracts for technology services and equipment in both the enterprise and its SBUs.
- Prepares quarterly and annual technology forecast reports.
- Develops and manages effective working relationships with other departments, groups, and personnel with whom work must be coordinated or interfaced.
- Assists in evaluating the technical staff of the enterprise and the SBU's user experience strategy functions.
- Maintains external links to other companies in the industry to gain competitive assessments and share information, where appropriate.
- Identifies the emerging user experience technologies to be assimilated, integrated, and introduced within the corporation which could significantly impact the enterprise's performance.
- Assesses new technologies to determine their potential value to the enterprise.
- Provides a source of specialized expertise that can serve the needs of other technical activities.
- Directs the administration and control of the research and development fund to gain the best possible return through innovative programs.

- Interfaces with external industrial and academic organizations to maintain state-of-the-art knowledge in emerging user experience technologies and to enhance the enterprise's image as a first-class corporation utilizing the latest thinking in all technology fields appropriate to the enterprise.
- Mandates and monitors the set of standards that support the user experience strategy.

Authority

- The CXO has the authority to recommend the purchase of equipment necessary for the user experience strategy (within the guidelines established by the enterprise).
- The CXO has the authority to engage external consultants as necessary to assist in all user experience strategy activities (within the guidelines established by the enterprise and IT).
- Hiring - The CXO will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all technology functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The CXO is responsible for oversight and review of staffing, projects, and performance of all user experience strategy functions of the organization.
- Contract Review - All contracts for user experience strategy are subject to a review by the CXO.

Contacts

Internal Contacts - The most frequent internal contracts are with the enterprise executive management, SBU senior management, the Chief Information Officer, and the technology staff of all SBUs.

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with user experience technology product and service companies is also made periodically.

Position Requirements

- 7-10 years leading innovation in small and mid-sized organizations.
- College degree in a related field.
- A visionary leader with change management experience.
- A strategic thought partner who has deep knowledge or experience in digital media with a strong command of digital media, audience trends, and outlook.
- An expert on modern forms of idea generation, product planning, development, and management.
- A proven track record leading a team and overseeing a portfolio of products and/or services that serve a specific purpose and targeted audiences as well as achieve measurable goals.
- An influencer who can diplomatically and persuasively communicate with a variety of individuals.

- A change agent who has shaped, shifted or changed the culture within an organization or who has implemented a unique approach that has had a measurable impact on teams.
- A leader of cross-functional or multi-disciplinary teams, bringing together individuals to achieve a common purpose and shared goals.
- A hands-on collaborator who can set, develop, and communicate strategies in a way that brings alignment, action, and excitement.
- A creative problem solver who has established accountability in an organization or to a team(s)
- Excellent verbal and written communication and strong interpersonal skills which inspire, motivate and bring people together.
- A CXO should have a background in business management and understand the language
- The individual should demonstrate initiative, exercise good judgment, exhibit a strong profit orientation, and can achieve results through others.
- Strong knowledge of, contracting, negotiating, organization development/change management, technology trends, the political and legislative process, strategic planning, action planning, and supervision are required for successful performance.
- Very strong conceptual, analytical, judgment, and communication abilities are critical.

Chief Experience Officer

JANCO ASSOCIATES, INC.

Chief Mobility Officer (CMO)

Position Purpose

The Chief Mobility Officer (CMO) is responsible for the overall direction of all mobility issues associated with Information Technology applications, communications (voice and data), and computing services within the enterprise. At the same time, the CMO must be aware of the implications of IT and industry mobility trends.

The CMO's role is to be the focal point for all mobility issues, including but not limited to enterprise applications, mobile devices, policies, and procedures, and oversee and review all mobility issues across the organization. As smartphones and tablets make their way into the workplace, much work remains to be done, not only in creating effective software but also in making them secure**.** This adds complexity to the role of this individual and drives the company's mobility initiatives. The CMO is the primary director of the development and implementation of policies and procedures to ensure that the organization's practices remain observant of all mandated local, state/province/county, and federal laws.

Develops guidelines for Work From Home (WFH) and all remote users. Both Internal and External to the enterprise.

Problems and Challenges

The CMO acts as staff to the CIO and CEO to help articulate the value of mobile for the enterprise and create the processes necessary to support the mobility initiative. The CMO, together with the CIO, is authorized to take all necessary actions to ensure the achievement of the objectives of the enterprise's mobility program including but not limited to BYOD and the firm's application store. Seamless integration of mobility management requirements including data and information from the customer through financial statements and management reporting is one of the primary challenges of this position

The major challenge for this individual is defining and managing the mobility issues of the enterprise with revenues over $(sales volume supported) per year while balancing security, privacy, and backup issues with financial and marketing needs.

This position requires management skills in directing a variety of projects in addition to an understanding of how mobility can be applied in all areas of the enterprise. The position requires supervisory/management experience and the flexibility to deal with people at a variety of levels; internally - enterprise staff, the board of directors, finance staff, other senior executive staff, and externally - auditors, media, employer groups, service providers, and industry associations.

Essential Position Functions

Principal Accountabilities

- CMO is the prime mover in the firm's mobility initiative, and as such provides guidance and direction to senior management on its implementation and is a sounding board for operational groups on how and where mobile solutions can be applied.
- Manages the development and implementation of the global mobility policy, standards, guidelines, and procedures.
- Develops a long-range mobility strategy for the enterprise.
- Develops plans for migration of mobility applications, processes, procedures, and policies to support necessary future directions of the enterprise.
- Identifies the emerging information technologies to be assimilated, integrated, and introduced within the enterprise.
- Directs the development and revisions of policies and procedures for the general operation of the mobility initiatives and their related activities. Including
    - Gaining visibility into the compliance of remote devices
    - Managing network security and sensitive information
    - Defining OS platforms and devices to support
    - Setting mobile policies
    - Managing BYOD
    - Resolving help desk incidents and problems
    - Ensuring compliance and producing audit trails
    - Supporting connectivity and Wi-Fi access
    - Installing and updating software
    - Approving applications available via the firm's application store
    - Enforcing mobile policies
    - Managing device security
- Coordinates with both internal and external audit groups to validate that the mobility users comply with published standards.
- Validates that the firm's and user's private and sensitive information is safe and secure
- Coordinates data, access, and applications across multiple channels within the firm's mobility initiative.
- Directs the design of mobile applications to support business processes that meet all security, backup, and compliance requirements.
- Is knowledgeable and complies with mandated security, disaster recovery and business continuity, internal control, and financial reporting requirements including, but not limited to, ISO, Sarbanes-Oxley, and HIPAA.
- Identifies potential areas of compliance vulnerability and risk; develops/implements corrective action plans for resolution of problematic issues, and provides general guidance on how to avoid or deal with similar situations in the future.

- Provides reports regularly, and as directed or requested, to keep the CIO, CEO, and other executive managers informed of the operation and progress of the mobility initiative.
- Ensures proper reporting of violations or potential violations to duly authorized enforcement agencies as appropriate and/or required.
- Works with the Human Resources Department and others as appropriate to develop an effective mobility training program, including appropriate introductory training for new employees as well as ongoing training for all employees and managers.
- Monitors the performance of the mobility initiative and relates activities continuingly, taking appropriate steps to improve its effectiveness.
- Conducts annual assessments.
- Identifies mobility goals and objectives consistent with the corporate strategic plan.
- Identifies key mobility initiative elements.
- Works with outside consultants as appropriate for independent mobility assessments.
- Provides a leadership role in the design and implementation of mobility procedures and processes in computer and communication hardware, operating system software, and productivity tools.
- Coordinates implementation plans, compliance product purchase proposals, and project schedules.
- Provides support to SBUs and external groups in the application of the enterprise's mobility policies.
- Defines the direction of in-house technical training seminars to improve overall employee awareness, response time, and ability to look into the future mobility opportunities of the enterprise.
- Participates in local and national user group presentations, and publishes articles describing enterprise activities and assessments of mobility opportunities and how they relate to the business.
- Develops and manages effective working relationships with other departments, groups, and personnel with whom work must be coordinated or interfaced.
- Assists in evaluating the technical staff of enterprise and SBU mobility functions.
- Maintains external links to other companies in the industry to gain competitive assessments and share information, where appropriate.
- Interfaces with external industrial and academic organizations to maintain state-of-the-art knowledge in emerging mobility issues and to enhance the enterprise's image as a first-class enterprise utilizing the latest thinking in this field.

Authority

- The CMO has the authority to recommend the implementation of and purchase of any of the equipment necessary for the mobility initiative of the enterprise. The CMO has the authority to engage external consultants as necessary to assist in large mobility projects (within the guidelines established by the enterprise).
- Hiring - The CMO will hire/terminate direct reports, as well as approve staff reporting to their direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all compliance functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The CMO is responsible for oversight and review of staffing, projects, and performance of all mobility initiatives of the organization.
- Contract Review - All contracts for related expenses and capital expenditures will be subject to a review by the CMO.

Contacts

Internal Contacts - The most frequent internal contracts are with the Board of Directors, Executive Management, Chief Information Officer, Chief Security Officer, and IT Staff of all SBUs. Also, there is significant contact with all functions within the enterprise including:

- Internal Legal Counsel
- Internal Audit
- Human Resources

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with information technology product and service companies is also made periodically. Also, there is significant contact with all external support functions of the enterprise including:

- External Legal Counsel
- External Audit
- Outsource Suppliers

Position Requirements

- A minimum of 10 years experience in an organization (within the same industry), including demonstrated leadership. Familiarity with operational, financial, quality assurance, and human resource procedures and regulations.
- Must be an intelligent, articulate, and persuasive leader who can serve as an effective member of the senior management team and who can communicate mobility-related concepts to a broad range of technical and non-technical staff.
- Should have experience with mobile technology, business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
- Must have a solid understanding of information technology and information security (including firewalls, VPNs, penetration testing, and other security devices.)
- Ability to work and effectively prioritize in a highly dynamic work environment.
- Experience with disaster recovery planning, testing, auditing, risk analysis, business resumption planning, contingency planning; TCP/IP firewalls, VPNs, and other security devices; as well as contract and vendor negotiation experience.
- Generally, a graduate degree in business or a related field together with significant executive experience and knowledge of the business industry is required. Strong knowledge of, contracting, negotiating, organization development/change management, technology trends, the political and legislative process, strategic planning, action planning, and supervision are required for successful performance. Very strong conceptual, analytical, judgment, and communication abilities are critical.

Chief Mobility Officer

Chief Security Officer (CSO)

Position Purpose

The Chief Security Officer (CSO) is responsible for the overall direction of all security functions associated with Information Technology applications, communications (voice and data), and computing services within the enterprise. At the same time, the CSO must be aware of the implications of legislated requirements that impact security for the enterprise. This includes but is not limited to Sarbanes Oxley Section 404 requirements and ISO 2000 Standards.

The CSO has the responsibility for global and enterprise-wide information security; he/she is also responsible for the physical security, protection services, and privacy of the corporation and its employees. Compliance with all mandated security and privacy requirements falls within the scope of this position.

The CSO oversees and coordinates security efforts across the enterprise, including information technology, human resources, communications, legal, facilities management, and other groups, to identify security initiatives and standards. The CSO works closely with the chief information officer and must have a strong working knowledge of information technology.

Problems and Challenges

The major challenge for this individual is defining and managing the security affairs of the enterprise with revenues over $(sales volume supported) per year while balancing security issues with financial and marketing needs. This is to be accomplished with the use of information and security technology that supports both self-generated enterprise growth and growth through acquisition. Seamless integration of security including data and information from the customer through financial statements and management reporting is one of the primary challenges of this position.

Security is a critical issue in the standardization of technology, applications, office automation, and workstations for the enterprise. As such, it is extremely important to the enterprise's current and future business operations. The Chief Security Officer (CSO) ensures the continued success of these areas while minimizing costs and maximizing equipment and employee performance.

This position requires time management skills in directing a variety of projects in addition to an understanding of how security is an issue within all areas of the enterprise. The position requires supervisory/management experience and the flexibility to deal with people at a variety of levels; internally - enterprise staff, the board of directors, finance staff, other senior executive staff, and externally - auditors, employer groups, service providers, and industry associations.

Essential Position Functions

Principal Accountabilities

- Oversees a network of security directors and vendors who safeguard the company's assets, intellectual property, and computer systems, as well as the physical safety of employees and visitors.
- Is knowledgeable and directs compliance with mandated security, disaster recovery and business continuity, internal control, and financial reporting requirements including ISO 27031, Sarbanes-Oxley, GDPR, CaCPA, and HIPAA.
- Manages all implications of mandated and regulated security requirements such as Sarbanes-Oxley.
- Works closely with both internal and external auditors.
- Conducts an annual threat and vulnerability assessment.
- Identifies protection goals and objectives consistent with the corporate strategic plan.
- Manages the development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Identifies key security program elements.
- Maintains relationships with local, state, and federal law enforcement and other related government agencies.
- Oversees the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.
- Understands and applies processes that support new governmental initiatives.
- Provides a leadership role in the design and implementation of security procedures and processes in computer and communication hardware, operating system software, and productivity tools.
- Manages development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Assists with the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Coordinates implementation plans, security product purchase proposals, and project schedules.
- Provides support to SBUs and external groups in the application of the enterprise's security policies.
- Develops plans for migration of security processes, procedures, and policies to support necessary future directions of the enterprise.
- Develops a long-range security strategy for the enterprise.
- Provides enterprise-wide direction for the use of security policies procedures and technologies for all enterprise operations, including other groups and subsidiaries.
- Defines new approaches for security technology including hardware, software, productivity tools, databases, CASE tools, image processing, and multimedia.

- Defines enterprise security objectives and plans to facilitate its orderly and efficient implementation.
- Provides direction to all security functions in computer and communication technology to maintain the maximum efficiency of the enterprise capital and human resources including hardware, software, and personnel.
- Defines security standards to ensure that all hardware, software, and database problems are solved in a timely and efficient manner including the computer and communication technology contribution to disaster recovery operations.
- Defines standards for security training, equipment cost and usage, cost/usage ratios, usage procedures, and technical personnel time/project allocation.
- Defines the direction of in-house technical training seminars to improve overall employee awareness, response time, and ability to look into the future security requirements of the enterprise.
- Maintains current knowledge of technical innovations in mainframe, minicomputer, LAN, WAN, and personal computing, and develops plans to utilize appropriate security technologies in support of future enterprise business expansion.
- Reviews cost estimates for security personnel requirements, new hardware, software upgrades or additions, and external consulting projects in support of other departments and SBUs.
- Participates in local and national user group presentations, and publishes articles describing enterprise activities and assessments of security and how they relate to the business.
- Interacts frequently with all SBU management on internal and external operations that are impacted by security issues both internal and external to the enterprise. This includes the review and approval of all major contracts for services and equipment in both the enterprise and SBUs Information Technology groups.
- Prepares quarterly and annual security forecast reports.
- Develops and manages effective working relationships with other departments, groups, and personnel with whom work must be coordinated or interfaced.
- Assists in evaluating the technical staff of enterprise and SBU security functions.
- Maintains external links to other companies in the industry to gain competitive assessments and share information, where appropriate.
- Identifies the emerging information technologies to be assimilated, integrated, and introduced within the enterprise which could significantly impact the enterprise's security.
- Assesses new security technologies to determine the potential value for the enterprise.
- Provides a source of specialized expertise that can serve the needs of other IT activities.
- Directs the administration and control of the security research and development fund to gain the best possible return through innovative programs.
- Interfaces with external industrial and academic organizations to maintain state-of-the-art knowledge in emerging security issues and to enhance the enterprise's image as a first-class enterprise utilizing the latest thinking in this field.
- Monitors the installed and planned-to-be-installed security processes and procedures.

- Monitors the set of standards that establish:
    - Mandatory security standards;
    - Security for classes of acquired equipment;
    - Documentation procedures for each security process and/ or procedure in place within the enterprise;
    - Identification of security processes/procedures maintenance standards; and
    - Examination of security procedures for all business functions developed as independent islands to ensure that they do not conflict with enterprise needs and that any necessary interfaces are constructed.

Authority

- The CSO has the authority to recommend the implementation of and purchase of any of the equipment necessary for the security of the enterprise's operations (within the guidelines established by the enterprise). The CSO has the authority to engage external consultants as necessary to assist in large security projects (within the guidelines established by the enterprise).
- Hiring - The CSO will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all security functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The CSO is responsible for oversight and review of staffing, projects, and performance of all security functions of the organization.
- Contract Review - All contracts for security-related computer and communication technology hardware, software, and services will be subject to a review by the CSO.

Contacts

Internal Contacts - The most frequent internal contracts are with the Chief Information Officer and IT staff of all SBUs. Also, there is significant contact with all functions within the enterprise including:

- Internal Legal Counsel
- Internal Audit
- Human Resources

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with information technology product and service companies is also made periodically. Also, there is significant contact with all external support functions of the enterprise including:

- External Legal Counsel
- External Audit
- Outsource Suppliers

Position Requirements

- This position requires a BS or BA degree in business or computer science with an emphasis on information technology and a minimum of eight to ten years of experience in computing and security, including experience with Internet technology and security issues. The position requires excellent verbal and written communication skills, previous leadership, management, and supervisory experience, and excellent time management abilities. The individual should demonstrate initiative, exercise good judgment, exhibit a strong profit orientation, and have the ability to achieve results through others. Included is the individual:
- Must be an intelligent, articulate, and persuasive leader who can serve as an effective member of the senior management team and who can communicate security-related concepts to a broad range of technical and non-technical staff.
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
- Should have some background in law, law enforcement, or intelligence. Must have a solid understanding of information technology and information security (including firewalls, VPNs, penetration testing, and other security devices.)
- Ability to work and effectively prioritize in a highly dynamic work environment.
- Experience with disaster recovery planning, testing, auditing, risk analysis, business resumption planning, contingency planning; TCP/IP firewalls, VPNs, and other security devices; as well as contract and vendor negotiation experience.
- Generally, a graduate degree in business or a related field together with significant executive experience and knowledge of the business industry is required. Strong knowledge of, contracting, negotiating, organization development/change management, technology trends, the political and legislative process, strategic planning, action planning, and supervision are required for successful performance. Very strong conceptual, analytical, judgment, and communication abilities are critical.

Data Protection Officer (DPO)

Position Purpose

The Data Protection Officer (DPO) is responsible for monitoring, informing, and advising the controller, the processor, and the employees who carry out the processing of their obligations according to the EU's General Data Protection Regulation (GPDR) and California's CaCPA.

The DPO monitors compliance with GPDR, with other EU or Member State data protection provisions, and with the policies of the controller or processor concerning the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations, and the related audits

The DPO must be aware of the implications of legislated requirements that impact security for the enterprise. This includes but is not limited to GPDR, Sarbanes Oxley Section 404 requirements, and ISO 2000 Standards.

The DPO has the responsibility for global and enterprise-wide data protection and compliance; he/she is also responsible for the physical security, protection services, and privacy of the corporation and its employees. The DPO works closely with the chief security officer and must have a strong working knowledge of information technology and enterprise operations.

Problems and Challenges

The major challenges for this individual include:

- Educating the company and employees on important compliance requirements
- Training staff involved in IT processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their data erased, and what measures the company has put in place to protect their personal information

Essential Position Functions

Principal Accountabilities

- Informs and advises the controller, the processor, and the employees who carry out the processing of their obligations according to GPDR and CaCPA.
- Monitors compliance with GPDR, with other EU or Member State data protection provisions, and with the policies of the controller or processor concerning the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations, and the related audits;
- Provides advice where requested as regards the data protection impact assessment and monitors its performance under GPDR requirements

- Conducts data protection impact assessments
- Conducts systematic monitoring of a publicly accessible area on a large scale.
- Makes public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to GPDR
- Makes public a list of the processing operations for which no data protection impact assessment is required.
- Communicates to executive management and the Board of Directors areas where there is or is not a data protection impact assessment
- Meets compliance requirements with approved codes of conduct
- Understands all of the risks associated with processing operations, taking into account the nature, scope, context, and purposes of the processing.
- Oversees a network of security directors and vendors who safeguard the company's assets, intellectual property, and computer systems, as well as the physical safety of employees and visitors.
- Is knowledgeable and directs compliance with mandated security, disaster recovery and business continuity, internal control, and financial reporting requirements including GPDR, ISO 27031, Sarbanes-Oxley, GDPR, CaCPA, and HIPAA.
- Manages all implications of mandated and regulated security requirements such as GPDR.
- Works closely with both internal and external auditors.
- Conducts an annual threat and vulnerability assessment.
- Identifies protection goals and objectives consistent with the corporate strategic plan.
- Manages the development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Maintains relationships with local, state, and federal law enforcement, EU GPDR groups, and other related government agencies.
- Oversees the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.
- Understands and applies processes that support new initiatives.
- Provides a leadership role in the design and implementation of security procedures and processes in computer and communication hardware, operating system software, and productivity tools.
- Manages development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Assists with the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Coordinates implementation plans, security product purchase proposals, and project schedules.
- Provides support to SBUs and external groups in the application of the enterprise's security policies.
- Develops a long-range security strategy for the enterprise.
- Provides enterprise-wide direction for the use of security policies procedures and technologies for all enterprise operations, including other groups and subsidiaries.
- Defines new approaches for security technology including hardware, software, productivity tools, databases, CASE tools, image processing, and multimedia.

- Defines enterprise security objectives and plans to facilitate its orderly and efficient implementation.
- Provides direction to all security functions in computer and communication technology to maintain the maximum efficiency of the enterprise capital and human resources including hardware, software, and personnel.
- Defines security standards to ensure that all hardware, software, and database problems are solved in a timely and efficient manner including the computer and communication technology contribution to disaster recovery operations.
- Defines standards for security training, equipment cost and usage, cost/usage ratios, usage procedures, and technical personnel time/project allocation.
- Defines the direction of in-house technical training seminars to improve overall employee awareness, response time, and ability to look into the future security requirements of the enterprise.
- Maintains current knowledge of technical innovations in mainframe, minicomputer, LAN, WAN, and personal computing, and develops plans to utilize appropriate security technologies in support of future enterprise business expansion.
- Reviews cost estimates for security personnel requirements, new hardware, software upgrades or additions, and external consulting projects in support of other departments and SBUs.
- Participates in local and national user group presentations, and publishes articles describing enterprise activities and assessments of security and how it relate to the business.
- Interacts frequently with all SBU management on internal and external operations that are impacted by security issues both internal and external to the enterprise. This includes the review and approval of all major contracts for services and equipment in both the enterprise and SBUs Information Technology groups.
- Prepares quarterly and annual security forecast reports.
- Develops and manages effective working relationships with other departments, groups, and personnel with whom work must be coordinated or interfaced.
- Assists in evaluating the technical staff of enterprise and SBU security functions.
- Maintains external links to other companies in the industry to gain competitive assessments and share information, where appropriate.
- Identifies the emerging information technologies to be assimilated, integrated, and introduced within the enterprise which could significantly impact the enterprise's security.
- Assesses new security technologies to determine the potential value for the enterprise.
- Provides a source of specialized expertise that can serve the needs of other IT activities.
- Directs the administration and control of the security research and development fund to gain the best possible return through innovative programs.
- Interfaces with external industrial and academic organizations to maintain state-of-the-art knowledge in emerging security issues and to enhance the enterprise's image as a first-class enterprise utilizing the latest thinking in this field.
- Monitors the installed and planned-to-be-installed security processes and procedures.

- Monitors the set of standards that establish:
    - Mandatory security standards;
    - Security for classes of acquired equipment;
    - Documentation procedures for each security process and/ or procedure in place within the enterprise;
    - Identification of security processes/procedures maintenance standards; and
    - Examination of security procedures for all business functions developed as independent islands to ensure that they do not conflict with enterprise needs and that any necessary interfaces are constructed.

Authority

- The DPO has the authority to recommend the implementation of and purchase of any of the equipment necessary for the security of the enterprise's operations (within the guidelines established by the enterprise). The DPO has the authority to engage external consultants as necessary to assist in large security projects (within the guidelines established by the enterprise).
- Hiring - The DPO will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all security functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The DPO is responsible for oversight and review of staffing, projects, and performance of all security functions of the organization.
- Contract Review - All contracts for security-related computer and communication technology hardware, software, and services will be subject to a review by the DPO.

Contacts

Internal Contacts - The most frequent internal contracts are with the Chief Information Officer and IT staff of all SBUs. Also, there is significant contact with all functions within the enterprise including:

- Internal Legal Counsel
- Internal Audit
- Human Resources

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with information technology product and service companies is also made periodically. Also, there is significant contact with all external support functions of the enterprise including:

- External Legal Counsel
- External Audit
- Outsource Suppliers

Position Requirements

This position requires a BS or BA degree in business or computer science with an emphasis on information technology and a minimum of eight to ten years of experience in computing and security, including experience with Internet technology and security issues. The position requires excellent verbal and written communication skills, previous leadership, management, and

supervisory experience, and excellent time management abilities. The individual should demonstrate initiative, exercise good judgment, exhibit a strong profit orientation, and have the ability to achieve results through others. Included is the individual:

a. Must be an intelligent, articulate, and persuasive leader who can serve as an effective member of the senior management team and who can communicate security-related concepts to a broad range of technical and non-technical staff.
b. Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
c. Should have some background in law, law enforcement, or intelligence. Must have a solid understanding of information technology and information security (including firewalls, VPNs, penetration testing, and other security devices.)
d. Ability to work and effectively prioritize in a highly dynamic work environment.
e. Experience with disaster recovery planning, testing, auditing, risk analysis, business resumption planning, contingency planning; TCP/IP firewalls, VPNs, and other security devices; as well as contract and vendor negotiation experience.
f. Generally, a graduate degree in business or a related field together with significant executive experience and knowledge of the business industry is required. Strong knowledge of, contracting, negotiating, organization development/change management, technology trends, the political and legislative process, strategic planning, action planning, and supervision are required for successful performance. Very strong conceptual, analytical, judgment, and communication abilities are critical.

Data Protection Officer

Manager BYOD Support

Position Purpose

The Manager BYOD Support is responsible for the overall coordination, control, and maintenance of all personal mobile devices within the enterprise to ensure compatibility and integration with enterprise strategies. The supervisor reports to the Director Technical Services.

Problems and Challenges

The Manager BYOD Support is challenged with establishing and maintaining a high level of creditability for the .function, enticing clients to consult with the function ensuring compatibility with enterprise strategies, and maximizing returns on investments. In meeting these challenges the Manager BYOD Support must constantly review, evaluate, plan, and budget activities in this dramatically and constantly evolving technological arena. Also, the manager must be cognizant of the latest releases of personal devices (hardware and software) and their security and application implications.

Essential Position Functions

Principal Accountabilities

- Identifies and initiates resolutions to user problems and concerns associated with mobile devices (including BYOD), hardware, and software to the user's satisfaction.
- Plans and coordinates the purchase, installation, and implementation of mobile devices hardware and software according to department standards and procedures.
- Analyzes the training needs of users, develops classroom curriculum, and provides quality individual and group training programs designed to ensure maximum utilization of all equipment, browsers, and operating systems.
- Maintains software and hardware registration and inventory to provide upgrades as necessary and ensure appropriate security levels are maintained.
- Upholds the enterprise policy guidelines as well as recommends new and improved guidelines to ensure compatibility and better serve users.
- Maintains current technical expertise in the rapidly changing technology of mobile devices.
- Utilizes state-of-the-art techniques when implementing hardware and software solutions.
- Interfaces with all of the various functions within IT and the enterprise to assure that the personal devices are utilized in a fashion that is consistent with the overall enterprise technology and business strategy.
- Prepares monthly status reports quantitatively reporting results of activities.
- Adheres to and maintains a positive working relationship with all enterprise departments to optimize working relationships and communication.
- Fulfills department requirements in terms of providing work coverage and administrative notification during periods of personal illness, vacation, or education.

- Performs at or above the enterprise's Information technology performance standard.

Authority

- Resolves problems directly with client BYOD, SmartPhones, laptops, and desktop hardware and software.
- Plans and coordinates hardware and software purchase and implementation.
- Develops training programs and curricula commensurate with needs.
- Works with users within the enterprise and with external vendors.

Contacts

Routine contact is required with IT application development and support personnel. Within the business, routine contact is required with end-user personnel.

Position Requirements

- BS or BA in business administration or computer science is desired
- 3 years of personal computer experience
- 2 years of experience in a training or support environment
- Strong written and verbal communication skills

Career Ladder

This position will lead to increased responsibilities in the information technology area. A specific managerial position above this one would be a manager in the Information Technology support function.

Manager BYOD Support

Manager Compliance

Position Purpose

The Manager Compliance is responsible for monitoring, informing, and advising the controller, the processor, and the employees who carry out the processing of their obligations according to all mandated compliance requirements including the EU's General Data Protection Regulation (GPDR).

The Manager Compliance monitors compliance for the protection of security and personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits

The Manager Compliance must be aware of the implications of legislated requirements that impact security for the enterprise. This includes but is not limited to GPDR, CaCPA, HIPPA, Sarbanes Oxley Section 404 requirements, and ISO 2000 Standards.

The Manager Compliance has the responsibility for global and enterprise-wide data protection and compliance; he/she is also responsible for the physical security, protection services, and privacy of the corporation and its employees. The Manager Compliance works closely with the chief security officer and must have a strong working knowledge of information technology and enterprise operations.

Problems and Challenges

The major challenges for this individual include:

- Educating the company and employees on important compliance requirements
- Training staff involved in Information Technology
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their data erased, and what measures the company has put in place to protect their personal information

Essential Position Functions

Principal Accountabilities

- Informs and advises the controller, the processor, and the employees who carry out the processing of their obligations according to compliance and privacy mandates.
- Monitors compliance data protection provisions and with the policies of the controller or processor for the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations, and the related audits;

- Provides advice where requested as regards the data protection impact assessment and monitors its performance according to compliance and privacy mandate requirements
- Conducts data protection impact assessments
- Conducts systematic monitoring of a publicly accessible area on a large scale.
- Makes public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to compliance and privacy mandates
- Makes public a list of the processing operations for which no data protection impact assessment is required.
- Communicates to executive management and the Board of Directors areas where there is or is not a data protection impact assessment
- Meets compliance requirements with approved codes of conduct
- Understands all of the risks associated with processing operations, taking into account the nature, scope, context, and purposes of the processing.
- Oversees a network of security directors and vendors who safeguard the company's assets, intellectual property, and computer systems, as well as the physical safety of employees and visitors.
- Is knowledgeable and directs compliance with mandated security, disaster recovery and business continuity, internal control, and financial reporting requirements including GPDR, CaCPA, HIPPA, Sarbanes Oxley Section 404 requirements, and ISO 2000 Standards.
- Manages all implications of mandated and regulated security requirements such as GPDR.
- Works closely with both internal and external auditors.
- Conducts an annual threat and vulnerability assessment.
- Identifies protection goals and objectives consistent with the corporate strategic plan.
- Manages the development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Maintains relationships with local, state, and federal law enforcement, EU GPDR groups, and other related government agencies.
- Oversees the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.
- Understands and applies processes that support new initiatives.
- Provides a leadership role in the design and implementation of security procedures and processes in computer and communication hardware, operating system software, and productivity tools.
- Manages development and implementation of global security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security.
- Assists with the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary.
- Coordinates implementation plans, security product purchase proposals, and project schedules.
- Provides support to SBUs and external groups in the application of the enterprise's security policies.
- Develops a long-range security strategy for the enterprise.

- Provides enterprise-wide direction for the use of security policies procedures and technologies for all enterprise operations, including other groups and subsidiaries.
- Defines new approaches for security technology including hardware, software, productivity tools, databases, CASE tools, image processing, and multimedia.
- Defines enterprise security objectives and plans to facilitate its orderly and efficient implementation.
- Provides direction to all security functions in computer and communication technology to maintain the maximum efficiency of the enterprise capital and human resources including hardware, software, and personnel.
- Defines security standards to ensure that all hardware, software, and database problems are solved in a timely and efficient manner including the computer and communication technology contribution to disaster recovery operations.
- Defines standards for security training, equipment cost and usage, cost/usage ratios, usage procedures, and technical personnel time/project allocation.
- Defines the direction of in-house technical training seminars to improve overall employee awareness, response time, and ability to look into the future security requirements of the enterprise.
- Maintains current knowledge of technical innovations in mainframe, minicomputer, LAN, WAN, and personal computing, and develops plans to utilize appropriate security technologies in support of future enterprise business expansion.
- Reviews cost estimates for security personnel requirements, new hardware, software upgrades or additions, and external consulting projects in support of other departments and SBUs.
- Participates in local and national user group presentations, and publishes articles describing enterprise activities and assessments of security and how they relate to the business.
- Interacts frequently with all SBU management on internal and external operations that are impacted by security issues both internal and external to the enterprise. This includes the review and approval of all major contracts for services and equipment in both the enterprise and SBUs Information Technology groups.
- Prepares quarterly and annual security forecast reports.
- Develops and manages effective working relationships with other departments, groups, and personnel with whom work must be coordinated or interfaced.
- Assists in evaluating the technical staff of enterprise and SBU security functions.
- Maintains external links to other companies in the industry to gain competitive assessments and share information, where appropriate.
- Identifies the emerging information technologies to be assimilated, integrated, and introduced within the enterprise which could significantly impact the enterprise's security.
- Assesses new security technologies to determine the potential value for the enterprise.
- Provides a source of specialized expertise that can serve the needs of other IT activities.
- Directs the administration and control of the security research and development fund to gain the best possible return through innovative programs.
- Interfaces with external industrial and academic organizations to maintain state-of-the-art knowledge in emerging security issues and to enhance the enterprise's image as a first-class enterprise utilizing the latest thinking in this field.
- Monitors the installed and planned-to-be-installed security processes and procedures.

- Monitors the set of standards that establish:
    - Mandatory security standards;
    - Security for classes of acquired equipment;
    - Documentation procedures for each security process and/ or procedure in place within the enterprise;
    - Identification of security processes/procedures maintenance standards; and
    - Examination of security procedures for all business functions developed as independent islands to ensure that they do not conflict with enterprise needs and that any necessary interfaces are constructed.

Authority

- The Manager Compliance has the authority to recommend the implementation of and purchase of any of the equipment necessary for the security of the enterprise's operations (within the guidelines established by the enterprise). The Manager Compliance has the authority to engage external consultants as necessary to assist in large security projects (within the guidelines established by the enterprise).
- Hiring - The Manager Compliance will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all security functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The Manager Compliance is responsible for oversight and review of staffing, projects, and performance of all security functions of the organization.
- Contract Review - All contracts for security-related computer and communication technology hardware, software, and services will be subject to a review by the Manager Compliance.

Contacts

Internal Contacts - The most frequent internal contracts are with the Chief Information Officer and IT staff of all SBUs. Also, there is significant contact with all functions within the enterprise including:

- Internal Legal Counsel
- Internal Audit
- Human Resources

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with information technology product and service companies is also made periodically. Also, there is significant contact with all external support functions of the enterprise including:

- External Legal Counsel
- External Audit
- Outsource Suppliers

Position Requirements

This position requires a BS or BA degree in business or computer science with an emphasis on information technology and a minimum of eight to ten years of experience in computing and security, including experience with Internet technology and security issues. The position requires excellent verbal and written communication skills, previous leadership, management, and supervisory experience, and excellent time management abilities. The individual should demonstrate initiative, exercise good judgment, exhibit a strong profit orientation, and have the ability to achieve results through others. Included is the individual:

- Must be an intelligent, articulate, and persuasive leader who can serve as an effective member of the senior management team and who can communicate security-related concepts to a broad range of technical and non-technical staff.
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
- Should have some background in law, law enforcement, or intelligence. Must have a solid understanding of information technology and information security (including firewalls, VPNs, penetration testing, and other security devices.)
- Ability to work and effectively prioritize in a highly dynamic work environment.
- Experience with disaster recovery planning, testing, auditing, risk analysis, business resumption planning, contingency planning; TCP/IP firewalls, VPNs, and other security devices; as well as contract and vendor negotiation experience.
- Generally, a graduate degree in business or a related field together with significant executive experience and knowledge of the business industry is required. Strong knowledge of, contracting, negotiating, organization development/change management, technology trends, the political and legislative process, strategic planning, action planning, and supervision are required for successful performance. Very strong conceptual, analytical, judgment, and communication abilities are critical.

Manager Record Administrator

Position Purpose

The Manager Record Administrator is responsible for managing, designing, and implementing the Record Management, Retention, and Destruction Program for the enterprise.

The Manager Record Administrator oversees the life cycle of records; develops standards for record creation, including permanent papers and records stored in electronic format; publishes records retention schedules and provides records management guidelines. The Manager Record Administrator publishes manuals, general letters, guidelines, and standards to keep the enterprise and its units informed about current records management issues and requirements.

Also, the Manager - Record Administrator provides records management guidelines for the enterprise and its various locations; publishes guidelines regarding archives and record storage vaults, and the creation of record retention and destruction schedules.

Problems and Challenges

The Manager Record Administrator is challenged with providing an optimal way to manage the record management system and meet all mandated needs associated with Sarbanes-Oxley.

Essential Position Functions

Principal Accountabilities

- Ensure compliance with federal, and state law, and regulatory agencies regarding the preservation of ENTERPRISE records.
- Ensure compliance with these standards and related record retention and disposition schedules.
- Jointly determine which ENTERPRISE records are Institutional records.
- Jointly develop and ensure the implementation of an organization and filing procedure for ENTERPRISE records.
- Jointly designate an original record custodian (ORC) from specific ENTERPRISE departments for Original Records. For example, the Procurement Department might be the ORC for Purchase Orders and Requisitions.
- Work with ENTERPRISE departments to develop departmental retention and disposition schedules for internal records not addressed in ENTERPRISE schedules.
- Work with the administrative services and records archivists to ensure that records scheduled for disposition are reviewed to determine if the records have to continue administrative or historical value. Records that have been determined as having such value shall be designated for archival retention and others will be properly disposed of.
- Work with the administrative services and records archivists to prepare and maintain a records management “manual” outlining procedures to:
    - Ensure the security of original records
    - Protect irreplaceable or vital records from destruction;

- Validate the Disaster Recovery Business and Continuity Plan complies with this policy (see http://www.e-janco.com/DisasterPlanning.htm)
- Designate original records custodians for new records;
- Ensure that original records are organized in an efficient and accessible manner;
- Ensure that original records are reviewed before disposal to determine whether they are archival records;
- Transfer records, in whole or in part, from the custodian of the original record to the appropriate archive;
- Provide periodic inventories of ENTERPRISE records; and
- Assist ENTERPRISE departments in complying with this standard and its schedules.

Authority

- Manages the Records Management System
- Coordinates all activities associated with the record management processes

Contacts

Contacts within the enterprise are with personnel associated with record creation, record use, and record destruction. Contact with outsiders as it relates to access to enterprise records.

Position Requirements

- A high school diploma is required
- Work towards a BS or BA degree in library science, record management or related technical field preferred, or a corresponding number of years experience in record management.
- Experience with physical and electronic record storage techniques
- Experience with record archival systems

Career Ladder

This position could lead to a managerial position with administrative services, information technology, or security administration.

Manager Record Administrator

Manager Security and Workstations

Position Purpose

The Manager Security and Workstations are responsible for the security of the enterprise's information technology data and processing assets including workstations that access those assets. Within the scope of this position is the planning, design, and implementation of security measures that safeguard access to the enterprise's facility and individual workstations that can access the enterprise's facility. The Manager Security and Workstations must provide a timely and rapid response to all reporting levels within the enterprise.

Internet and Intranet security fall within the scope of responsibilities for this position. Also, if any of the enterprise's operations are outsourced, this individual is the focal point for security both within the enterprise and the outsourced functions. This includes responsibility for all network-related security issues such as firewalls, routers, and password control.

The Manager Security and Workstations are tasked with the development, implementation, and compliance with all security policies and procedures, including PC-DSS and ISO 2000 as implemented within the enterprise.

Problems and Challenges

The Manager Security and Workstations have the challenge of protecting the enterprise's facility and workstation assets from intentional or accidental access, copying, destruction, or modification. This will minimize the impact on those who need legitimate access to the enterprise's electronic assets. The Manager needs to be cognizant of the security requirements of Sarbanes-Oxley.

Problems and challenges associated with WFH users for both security and compliance mandates are to be addressed by this individual.

Essential Position Functions

Principal Accountabilities

- Establishes, maintains, and monitors all log-on identifications and access rules, defining specific access to network, files, and database management systems. The methodical generation of such a system shall consolidate disparate application security systems under one methodology.
- Complies with the record management policy including record retention and record destruction.
- Validates BYODs comply with all security and compliance requirements.
- Reviews the compliance of the enterprise's security guidelines in concert with the Chief Security Officer to ensure that all mandated security requirements are met.
- Recommends modification of the enterprise's security guidelines to the Chief Security Officer.
- Recommends security software and its application to all storage device types and access to them for classified and unclassified areas.

- Establishes alternative security measures, if needed, to support disaster recovery efforts.
- Recognizes and identifies potential areas where existing data security policies and procedures require change, or where new ones need to be developed, especially regarding future business expansion.
- Maintains contact with vendors regarding security system updates and technical support of security products.
- Prepares recommendations and implements changes to work methods and procedures to make them more effective and/or to strengthen security measures.
- Provides management with risk assessments and information security training to uphold enterprise security measures.
- Analyzes the work unit, making recommendations to improve workflow efficiency and/or operation productivity.
- Manages Internet and Intranet security-based issues. This includes firewalls, routers, and port accessibility.
- Informs management of critical issues that may affect clients and completes status and statistical reports in the assigned area as required.
- Recognizes and identifies potential areas where existing policies and procedures require change, or where new ones need to be developed, especially regarding future business expansion.
- Fulfills departmental requirements in terms of providing work coverage and administrative notification during periods of personal absence.
- Performs at or above the enterprise's Information Technology evaluation standards.
- Trains, supervises, assigns staff to projects, evaluates, and is responsible for hiring/termination of staff to maintain the optimum performance of job duties.

Authority

- Identify potential service-level problems before they occur and implement solutions.
- Direct self and the activity of others during the design and implementation of data security measures.
- Monitors compliance with the security guidelines for use of the enterprise's electronic assets via local and remote workstations.
- Schedule and prioritize activities to accommodate the enterprise's operational, IT, and customer needs while minimizing the impact on the enterprise.
- Maintain and documents data security measures within the enterprise and recommend security software packages and/or upgrades.
- Contribute to the training and development of IT personnel in direct support of IT delivery of services.

Contacts

Routine contact is required with other IT managers and staff personnel at all organizational levels to develop, implement, maintain, and enforce security methods and measures. Within the

enterprise, periodic contact is required with executives in charge of the key business units using IT services.

Position Requirements

- High school diploma or equivalent
- BS or BA degree in computer science or related field preferred, or a corresponding number of years experience in data security
- 4 years experience in data security, with 2 years in a managerial position with the ability to plan and control projects
- Knowledge at the expert level of current techniques and hardware capabilities of a large-scale database and data communications environment
- Ability to understand, and relate to other members of the organization, technical manuals, software specifications, hardware principles of operations, and general methods of systems software operations and security
- Ability to communicate effectively dealing with internal and external customers and suppliers

Career Ladder

The Manager Security and Workstations may progress to Manager Administration and Facilities.

JANCO ASSOCIATES, INC.

Manager Social Networking

Position Purpose

The Social Media Manager will administer the company's social media marketing and advertising. Administration includes but is not limited to:

- Deliberate planning and goal setting
- Development of brand awareness and online reputation
- Content management
- SEO (search engine optimization) and generation of inbound traffic
- Cultivation of leads and sales

The Manager Social Networking directs community management, and content creation, and executes social media programs across all the enterprise's social media channels to support the enterprise's brand. The Manager Social Networking communicates with the public through platforms that allow users to create and share content online. The Manager Social Networking directs the nurturing of a growing audience of fans and followers. Through social media activities, the Manager Social Networking will build more brand awareness, a consideration that ultimately will drive more sales for the enterprise.

The Manager Social Networking is not only a brand and product line expert, but also a seasoned technology expert. The Manager Social Networking is responsible for the adoption of social media technologies across the entire business.

Problems and Challenges

The major challenge for this individual is defining the social media presence of the enterprise's brands and products while balancing digital assets and computing services with financial and marketing needs. This is accomplished with the use of technology that supports both self-generated brand awareness and growth. Seamless integration of social media and marketing assets from the customer, through product and service design, financial statements, and management reporting is a primary concern.

Social media presence is the focal point for this position within the enterprise. The Manager Social Networking ensures the continued success of these areas while simultaneously minimizing costs and maximizing marketing and advertising performance.

Challenges include:

- Earning company-wide commitment - Getting everyone on board with the digital vision is a major endeavor task with internal politics and an ever-changing digital landscape.
- Working with senior and executive management in developing a social media presence mission statement – Manager Social Networking is responsible for end-to-end implementation of the company's social media presence in concert with the company's long-term marketing and external image strategy.
- Creating a bridge between social media and brand management – the Manager Social Networking focus is the relationship between the brand and the customer.
- Maintaining links with experts.
- Maintaining a balance between enterprise management and technology.
- Connecting social media investments to enterprise KPIs statements achieve positive brand performance.

Essential Position Functions

The Social Media Manager is a highly motivated, creative individual with experience and a passion for connecting with current and future customers. That passion comes through as he/she engages with customers daily, with the ultimate goal of turning fans into customers.

Community leadership and participation (both online and offline) are integral to a Social Media Manager's success. An essential component is communicating the company's brand in a positive, authentic way that will attract today's modern, hyper-connected buyers.

The Social Media Manager is instrumental in managing the company's content-related assets. Google's #1 search ranking factor is relevant content (content that serves the searcher's needs the best).

Principal Accountabilities

- **Social Media – Editorial Management**
  - Plans and executes social editorial calendars in partnership with internal stakeholders and external agencies. (Annual, Quarterly, and Monthly)
  - Creates monthly editorial content calendars and shares with internal/external stakeholders.
  - Ensures that communication is properly aligned with overall business goals and internal/external stakeholders and that it is timely and contextually relevant.
  - Plans and executes content publication for the enterprise on all owned social media channels including Facebook, Twitter, Instagram, Pinterest, and emerging social media channels.
  - Creates and reviews the copy for all social media channels while ensuring the voice and tone are aligned with the brand style guide.
  - Develops high-quality social media content. This includes working with influencers, building a library of image assets, and supporting video production.
- **Social Media – Community Management**
  - Reacts to messages daily by answering questions, creating dialogues, and fostering relationships with the enterprise's social community.
  - Routes questions/topics to proper internal/ external stakeholders.
  - Supports Digital Brand Manager in managing social media crisis and execution.
- **Social Media – Analytics**
  - Measures and reports on performance, ensuring key learnings are cascaded to cross-functional teams regularly (Monthly, Quarterly, and Annually). This includes reporting on engagement, community size, specific campaigns, or programs. Share with internal/external stakeholders.
  - Execute social listening, conversation, and sentiment analysis to help measure the impact of marketing communications and identify trends/opportunities for the business.
- **Social Media – Best Practices and Processes**
  - Support social listening and escalation in partnership with consumer relations, as well as conversation and sentiment analysis to help measure the impact of marketing communications and identify trends/opportunities for the business.
  - Lead and establish social media best practices and socialize with all stakeholders.

- Acts as the internal social media expert, share knowledge of the digital space with teams, host review meetings, and learning sessions
- Acts as an internal social media consultant to support collaboration and expansion of activities
- Develops community guidelines for main channels such as Facebook.
- Develops the internal social media playbook.
- Leads and refines community management processes at the enterprise while collaborating with cross-functional teams.
- Focuses on ROI and KPI in the digital asset management processes

- **Social Media Campaigns**
  - Has a significant role in consulting on and executing all social media campaigns in partnership with brand management.
  - Advises on the individual campaign and total the enterprise's social media strategies to ensure all appropriate trends and tactics are considered/applied.
  - Manages social media creative development
  - Ensures prioritization and consistency between the campaign and other enterprise strategies
  - Has responsibility for making sure a systematic approach to both planning and reporting is implemented.
  - Works with the Digital Brand Manager on defining and planning the social media KPIs and ensuring these are set accurately.
  - Works with the Digital Brand Manager and agency partners to analyze cross-campaign performance to draw insights that can be applied to refine future programs.
  - Ensures assets are optimized to drive campaign objectives.
  - Supports “Always-On’ paid social content is being seen by the right consumers on the right channel on the right device at the right time.
  - Ensures campaigns have appropriate social media activations that are on strategy and optimized for the social channel.
- **Digital Marketing Campaigns and Website**
  - Supports digital marketing activities as needed.
  - Supports tracking and management of ongoing updates to web content as needed.
  - Supports the troubleshooting of digital efforts as needed.
- **Innovation/Emerging Technology**
  - Helps the marketing team to innovate through influencer programs.
  - Helps the marketing team to maximize the way they use and think about data.
  - Fosters a culture of “Test and Learn” within our marketing team.
  - Identifies opportunities to try new things and evaluates effectiveness. Scale if successful, move on if not.
  - Take advantage of the enterprise's location to foster relationships with external technology companies.
  - Expands our network to provide access to new, interesting opportunities.

Authority

- The Manager Social Networking has the authority to recommend the purchase of equipment necessary for the brand management strategy (within the guidelines established by the enterprise).
- The Manager Social Networking has the authority to request external consultants as necessary to assist in all social networking strategy activities (within the guidelines established by the enterprise and IT).
- Hiring - The Manager Social Networking will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all technology functions within the enterprise including the SBUs that may not directly report to this position.
- Budgetary - The Manager Social Networking is responsible for oversight and review of staffing, projects, and performance of all digital strategy functions of the organization.
- Contract Review - All contracts for digital strategy are subject to a review by the Manager Social Networking.

Contacts

Internal Contacts - The most frequent internal contracts are with the Vice President Marketing, Digital Brand Manager, enterprise executive management, SBU senior management, the Chief Information Officer, and technology staff of all SBUs.

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with social media technology product and service companies is also made periodically.

Position Requirements

- Experience in Social Media Marketing and Integrated Marketing
- Excellent verbal & written communication skills – must be able to translate new digital concepts to various stakeholders, and write engaging consumer-facing content.
- Familiarity with social media analytics & measurements.
- Critical eye for design; high standards for content quality
- Collaborative, team-oriented spirit with a history of success developing cross-functional relationships & leading cross-functional projects
- Ability to plan across social media channels, then execute with discipline
- Ability to align priorities towards a forward-moving body of work centered on Business goals (Awareness, Acquisition, Conversion, etc.)
- Experience & comfort managing day-to-day communication with third-party vendors and key partners (e.g. resolve issues, document challenges, create roadmaps, facilitate collaborative brainstorming sessions, etc.)
- Strong project management skills
- Computer Experience: Basic HTML Coding, CMS tools, Adobe Creative Suite, Social Listening/Analytics Platforms, JavaScript, Salesforce/other ESP, E-commerce experience a plus

- The Manager Social Networking should have a background in business management and understand the language of financial statement analysis, ROI, KPIs, and change management.
- College degree (BA or BS); background in Marketing, Communications, Public Relations, Business, Computer Science or related field. MBA preferred.
- 2+ years of social media marketing
  - 1-2 years of experience managing multiple social media channels
  - 1-2 years experience managing PPC campaigns
  - 1-2 years experience managing websites, coordinating web projects and email campaigns (agency experience helpful)
- Has excellent verbal and written communication skills, previous leadership,
- Has strong conceptual, analytical, judgment, and communication abilities.

Career Ladder

The Manager Social Networking can fill a senior IT position or marketing within the enterprise. Beyond this lateral movement, the logical promotional progression would be into the Brand Management position.

Manager Social Networking

Manager Telecommuting

Position Purpose

The Manager Telecommuting oversees telecommuting activities, including the integration of applications – both internal and external to the enterprise, file management and site maintenance, database management, coordination of the retrieval of pertinent information from the site to telecommuters, and archiving and record management. The Manager Telecommuting reporting relationships vary by organization.

This individual champions the conceptualization and implementation of all telecommuting within the enterprise.

Problems and Challenges

The Manager Telecommuting is challenged with managing technical support for problems related to internal and external telecommuting activities, as well as performing total quality management of telecommuting applications, including aesthetic consistency, evaluation of links, and usability.

Essential Position Functions

Principal Accountabilities

- Manages the installation, configuration, and maintenance of telecommuting components of the IT infrastructure to ensure proper transmission of documents and files over current protocols.
- Defines and manages the standards for the enterprise. May need to evaluate competing for hardware and software to decide on needs within the enterprise.
- Defines and sets network security layers (firewalls) to deter unauthorized access to proprietary data.
- Manages the implementation and operation of all telecommuting security with a password and digital encryption information for secured documents.
- Researchs and implements security policies.
- Ensures the definition of the look and feel of the enterprise sites is consistent with the enterprise.
- Specifies standards for enterprise-wide (intranet) Web documents, ensures that all submitted documents meet those standards, and converts all other submitted materials to Web documents.
- Manages the enterprise's data exchange and integrates multimedia assets and database applications.
- Coordinates overall site design implementation with creative staff, to match the desired outcome with technological feasibility.
- Generates timely reports as required.
- Secures website design, programming, graphics word-processing, and authoring support as needed.

- Manages the programming of telecommuting applications in all common Web HTML formatting tools such as animated GIF and Java. This includes Web page-to-data access routines using the common gateway Interface.
- Coordinates scripting and programming with other IT authors.
- Integrates new technologies (add-ins and plug-ins) into the telecommuting environment.
- Maintains cross-platform and cross-browser compatibility.
- Identifies the necessary training and education requirements.
- Researches new telecommuting features and tools which might be useful for authoring documents, managing the telecommuting environment, and for expanding online offerings.
- Mediates between the business needs, content authors, and system administrator, ensuring adherence to applicable Web language coding standards and currency of Weblinks.
- Optimizes telecommuting architecture for navigability by taking editorial ownership of the content, quality, and style of the site. Consults with graphic artists as required.
- Provides first-level help desk support on telecommuting issues.
- Defines the standards for a consistent visual image through uniform fonts, formatting, icons, images, and layout techniques.
- Defines appropriate resolutions, sizes, color maps, and depths to ensure that images are delivered at sufficiently high speed and quality for intended output media.
- See that all personnel are trained in the use and applications associated with the Intranet, Web pages, uploading of data; file transfer; image acquisition using optical scanners and imaging tools.
- Approves all final submissions for visual congruity and proper coding in a common programming language.

Authority

- Depending on the maturity of the position (see Position Purpose above), a Manager Telecommuting should have the authority to direct the overall content of telecommuting, at least in matters of style, wording, and overall look and feel.
- The Manager Telecommuting is a direct report to a member of senior management; he or she will often “inherit” certain measures of authority from that manager in all ways except the setting of policy.

Contacts

Contacts within the enterprise may cut across all levels but will be seen primarily to concentrate on telecommuters and senior management, including an oversight committee, if one exists. Contacts external to the enterprise typically include vendors, suppliers, hardware and software manufacturers, developers, Web resource providers, and other managers.

Position Requirements

- A high school diploma is required
- BS or BA degree in computer science, graphic design, or related work experience is desirable
- Ability to work within a variety of Web-based hardware environments, and to manage the website from a client as well as a server perspective
- Ability to produce Web pages that are aesthetically pleasing within the limitations of the delivery medium
- Experience with server platforms and Web server software, networking, and security architecture and implementation
- Familiarity with standard Internet protocols and other Internet issues such as name servers, hypertext transfer, file transfer, e-mail, Usenet, etc.
- Familiarity with common Web languages and extensions as required, e.g. tables, frames, server-push/client-pull, server-side includes, etc., as well as awareness of browser compatibility issues
- Familiarity with both Telecommuting connectivity protocols and software
- Working knowledge of graphics applications allowing full manipulation of files
- Experience with database design and implementation utilizing databases
- Familiarity with Internet connectivity hardware (modems, data service units/channel service units, routers, terminal servers)
- Experience with Web Server-to-email interfaces
- Should be familiar with Common Gateway Interface and Java language programming, as well as animated GIF creation
- Ability to program forms and implement scripts
- Ability to interact positively and effectively with employees at all levels within the organization, as well as with customers, prospects, and vendors
- Demonstrate project management skills
- Excellent oral and writing skills

Career Ladder

The Manager Telecommuting position will stabilize as a medium- to high-ranking staff position, with a path to a management position such as Manager Network Services.

Manager Telecommuting

Manager WFH Support

Position Purpose

The Manager WFH Support oversees work from home activities, including the integration of connectivity and applications. This includes both internal and external to the enterprise, file management, site maintenance, database management, mandated compliance requirements, security management, and coordination of the retrieval of pertinent information from the site to WFHers in the operation of their enterprise roles. The Manager WFH Support reporting relationships vary by organization.

This individual champions the conceptualization and implementation of all WFH activities within the enterprise. Also, the individual provides front-line support for all WFH activities.

Problems and Challenges

The Manager WFH Support is challenged with managing technical support for problems related to internal and external telecommuting activities, as well as performing total quality management of telecommuting applications, including aesthetic consistency, evaluation of links, and usability.

An added challenge is validating compliance with OSHA and the enterprise's safety program.

Essential Position Functions

Principal Accountabilities

- Manages the installation, configuration, and maintenance of WFH components of the IT infrastructure to ensure proper transmission of documents and files over current protocols.
- Supports all connectivity issues associated with WFH sites including broadband and Wi-Fi interactions with suppliers of those services.
- Defines and manages the standards for the enterprise. May need to evaluate competing for hardware and software to decide on needs within the enterprise.
- Defines and sets network security layers (firewalls) to deter unauthorized access to proprietary data.
- Manages the implementation and operation of all WFH security with password and digital encryption information for secured documents.
- Researchs and implements security policies.
- Ensures the definition of the look and feel of the enterprise sites is consistent with the enterprise.
- Specifies standards for enterprise-wide (intranet) Web documents, ensures that all submitted documents meet those standards, and converts all other submitted materials to Web documents.
- Manages the enterprise's data exchange and integrates multimedia assets and database applications.

- Coordinates overall site design implementation with creative staff, to match the desired outcome with technological feasibility.
- Generates timely reports as required.
- Secures website design, programming, graphics word-processing, and authoring support as needed.
- Manages the programming of telecommuting applications in all common Web HTML formatting tools such as animated GIF and Java. This includes Web page-to-data access routines using the common gateway Interface.
- Integrates new technologies (add-ins and plug-ins) into the WFH environment.
- Maintains cross-platform and cross-browser compatibility.
- Identifies the necessary training and education requirements.
- Researches new WFH features and tools which might be useful for managing the WFH environment, and for expanding online offerings.
- Optimizes WFH and the general telecommuting architecture for navigability by taking editorial ownership of the content, quality, and style of the site. Consults with graphic artists as required.
- Provides first-level help desk support on WFH issues.
- Defines the standards for a consistent visual image through uniform fonts, formatting, icons, images, and layout techniques.
- See that all personnel are trained in the use and applications associated with the Intranet, Web pages, uploading of data; file transfer; image acquisition using optical scanners and imaging tools.

Authority

- Depending on the maturity of the position (see Position Purpose above), a Manager WFH Support should have the authority to direct the overall content of the WFH environment.
- The Manager WFH Support is a direct report to a member of senior management; he or she will often “inherit” certain measures of authority from that manager.

Contacts

Contacts within the enterprise may cut across all levels but will be seen primarily to concentrate on WFH employees, telecommuters, and senior management, including an oversight committee, if one exists. Contacts external to the enterprise typically include vendors, suppliers, hardware and software manufacturers, developers, Web resource providers, and other managers.

Position Requirements

- A high school diploma is required
- BS or BA degree in computer science, graphic design, or related work experience is desirable
- Ability to work within a variety of hardware environments, and to manage WFH from a client as well as a server perspective
- Experience with server platforms and Web server software, networking, and security architecture and implementation
- Familiarity with standard Internet protocols and other Internet issues such as name servers, hypertext transfer, file transfer, e-mail, Usenet, etc.
- Familiarity with common Web languages and extensions as required, e.g. tables, frames, server-push/client-pull, server-side includes, etc., as well as awareness of browser compatibility issues
- Familiarity with both WFH and Telecommuting connectivity protocols and software
- Working knowledge of graphics applications allowing full manipulation of files
- Experience with database design and implementation utilizing databases
- Familiarity with Internet connectivity hardware (modems, data service units/channel service units, routers, terminal servers)
- Experience with Internet-based server-to-email interfaces
- Ability to interact positively and effectively with employees at all levels within the organization, as well as with customers, prospects, and vendors
- Demonstrate project management skills
- Excellent oral and writing skills

Career Ladder

The Manager WFH Support position will stabilize as a medium to a high-ranking staff position, with a path to other senior management positions.

Manager WFH Support

Record Management Coordinator

Position Purpose

Under general supervision, the Record Management Coordinator is responsible for maintaining centralized records in the enterprise and for supervising the work of employees engaged in processing records; performs a variety of difficult clerical tasks, and does related work as required.

Problems and Challenges

Distinguished from Secretary and Typist Clerk in that the Record Management Coordinator has overall responsibility for the management and maintenance of centralized enterprise records. Distinguished from the Records Supervisor in other departments in that the incumbent is not responsible for records maintained within those departments.

The WFH environment must be addressed with specific guidelines and validation for compliance.

Essential Functions

Principal Accountabilities

- Establishes, maintains, and updates complex computerized database programs and manual filing systems for centralized enterprise records.
- Complies with all mandated compliance requirements and ensures the enterprise's security and privacy policies are followed
- Establishes procedures for data entry, data integrity, and indexing, tracking, and retrieving records.
- Receives, indexes enter, stores, retrieves, films, and destroys records in keeping with enterprise policies, State, and Federal requirements.
- Maintains a vital records program, and updates and maintains a records retention program.
- Prioritizes work.
- Supervises, trains, and works with subordinate staff in maintaining records, and keeping records of work performed.
- Provides documents, records, and information to enterprise personnel and the general public, and researchs requested information as necessary.
- Works with and advises departments on the proper procedures for preserving, storing, retrieving, retaining, and destroying records following established policies.

- Diagnoses and resolves computerized filing system problems through consultation with the appropriate enterprise contacts and outside vendors.
- Designs, maintains, and updates storage areas to ensure the most effective use of space.
- Coordinates the installation, modification, and updating of computerized record systems.
- Operates document imaging equipment, microfilm reader/printers, load lifters, computers, and printers.
- Coordinates microfilming of records by vendors and other work related to records maintenance.
- Develops procedures and standards for the archiving and retention of historical records and documents.
- Assists with daily operations and performs office duties as necessary.

Authority

- Manages the Records Management System
- Coordinates all activities associated with the record management processes

Contacts

Contacts within the enterprise are with personnel associated with record creation, record use, and record destruction. Contact with outsiders as it relates to access to enterprise records.

Position Requirements

- Three years of increasingly responsible records management experience or administrative experience involving filing systems. Coursework in records management and computerized filing systems is preferred. Designation as a Certified Records Manager (CRM) is desirable.
- Work towards a BS or BA degree in library science, record management, or a related technical field preferred, or a corresponding number of years of experience in record management.
- Experience with physical and electronic record storage techniques
- Experience with record archival systems

Career Ladder

This position could lead to a managerial position as a Manager Record Administrator or manager in administrative services, information technology, or security administration.

Security Architect

Position Purpose

The Security Architect, under the direction of the Manager Network Services, assumes responsibility for data security including the planning, design, and implementation of security measures that safeguard access to enterprise terminal files and data elements. The administrator provides rapid response to the user community's request for security assistance.

The Security Architect secures enterprise information by determining security requirements; planning, implementing, and testing security systems; preparing security standards, policies, and procedures; mentoring team members.

Problems and Challenges

The challenge facing the Security Architect is the total security of data relating to the enterprise's applications and architecture.

Essential Position Functions

Principal Accountabilities

- Complies with all mandated compliance requirements and ensures the enterprise's security and privacy policies are followed.
- Enhances security team accomplishments and competence by planning the delivery of solutions; answering technical and procedural questions for less experienced team members; teaching improved processes; mentoring team members.
- Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates.
- Plans security systems by evaluating network and security technologies; developing requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related security and network devices; designs public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures as well as hardware and software; adhering to industry standards.
- Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation.
- Verifies security systems by developing and implementing test scripts.
- Maintains security by monitoring and ensuring compliance with standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs.
- Upgrades security systems by monitoring the security environment; identifying security gaps; evaluating and implementing enhancements.

- Prepares system security reports by collecting, analyzing, and summarizing data and trends.
- Updates job knowledge by tracking and understanding emerging security practices and standards; participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.
- Enhances department and organization reputation by accepting ownership for accomplishing new and different requests; exploring opportunities to add value to job accomplishments.
-
- Establishes, maintains, and monitors all log-on identifications and access rules, defining specific access to network, files, and database management systems. The methodical generation of such a system shall consolidate disparate application security systems under one methodology.
- Recommends security software and its application to all storage device types and access to them.
- Establishes alternative security measures if needed to support disaster recovery efforts.
- Recognizes and identifies potential areas where existing data security policies and procedures require change, or where new ones need to be developed, especially regarding future business expansion.
- Participates with vendors in the assessment of advanced data security systems.
- Fulfills departmental requirements in terms of providing work coverage and administrative notification during periods of personal illness, vacation, or education.
- Performs at or above the enterprise's Information Technology performance standards.

Authority

- Design and implement data security measures within the enterprise.
- Maintain and document data security measures within the enterprise.
- Recommend security software packages and/or upgrades.

Contacts

Routine contact is required with IT managers at all organizational levels and with technology vendors. Within the business, periodic contact is required with executives in charge of the key business units using IT services.

Position Requirements

- A high school diploma is required
- BS or BA degree in computer science, business administration, or related work experience
- 5 years experience in Information Technology, 2 years within the data security
- Strong working knowledge of operating systems, job control languages (or other production control languages), utilities, and security environment software
- Programming and/or network experience desirable
- Good oral and written communications skills
- Service-oriented and work easily with users and IT management

Career Ladder

The logical career progression for the Security Architect would be to advance into the position of Manager Network Services.

Social Media Specialist

Position Purpose

The Social Media Specialist leads community management, content creation, and executes social media programs across all the enterprise's social media channels to support the enterprise's brand. The Social media specialist communicates with the public through platforms that allow users to create and share content online. They run their employers' social media accounts, working to build a brand's reputation.

The Social Media Specialist nurtures a growing audience of fans and followers. Through social media activities, the social media specialist will build more brand awareness, a consideration that ultimately will drive more sales for the enterprise.

The individual has experience in social media, is enthusiastic about both the creative and analytical side of social media programs, and also has a pulse on the latest trends. The Social Media Specialist drives engagement on all platforms, they monitor communities and nurture relationships with the enterprise's fans while managing any issue that may occur.

The Social Media Specialist is not only a brand and product line expert, but also a seasoned technology expert. The Social Media Specialist is responsible for the adoption of social media technologies across the entire business.

Problems and Challenges

The major challenge for this individual is defining the social media presence of the enterprise's brands and products while balancing digital assets and computing services with financial and marketing needs. This is accomplished with the use of technology that supports both self-generated brand awareness and growth. Seamless integration of social media and marketing assets from the customer, through product and service design, financial statements, and management reporting is a primary concern.

Social media presence is the focal point for this position within the enterprise. The Social Media Specialist ensures the continued success of these areas while simultaneously minimizing costs and maximizing marketing and advertising performance.

Challenges include:

- Earning company-wide commitment - Getting everyone on board with the digital vision is a major endeavor task with internal politics and an ever-changing digital landscape.
- Working with senior and executive management in developing a social media presence mission statement – Social Media Specialist is responsible for end-to-end implementation of the company's social media presence in concert with the company's long-term marketing and external image strategy.
- Creating a bridge between social media and brand management – the Social Media Specialist's focus is the relationship between the brand and the customer.
- Maintaining links with experts.
- Maintaining a balance between enterprise management and technology.
- Connecting social media investments to enterprise KPIs to achieve positive brand performance.

Essential Position Functions

Principal Accountabilities

- **Social Media – Editorial Management**
  - Plans and executes social editorial calendars in partnership with internal stakeholders and external agencies. (Annual, Quarterly, and Monthly)
  - Creates monthly editorial content calendars and shares with internal/external stakeholders.
  - Ensures that communication is properly aligned with overall business goals and internal/external stakeholders and that it is timely and contextually relevant.
  - Plans and executes content publication for the enterprise on all owned social media channels including Facebook, Twitter, Instagram, Pinterest, and emerging social media channels.
  - Creates and reviews the copy for all social media channels while ensuring the voice and tone are aligned with the brand style guide.
  - Develops high-quality social media content. This includes working with influencers, building a library of image assets, and supporting video production.
- **Social Media – Community Management**
  - Reacts to messages daily by answering questions, creating dialogues, and fostering relationships with the enterprise's social community.
  - Routes questions/topics to proper internal/ external stakeholders.
  - Supports Digital Brand Manager in managing social media crisis and execution.
- **Social Media – Analytics**
  - Measures and reports on performance, ensuring key learnings are cascaded to cross-functional teams regularly (Monthly, Quarterly, and Annually). This includes reporting on engagement, community size, specific campaigns, or programs. Share with internal/external stakeholders.
  - Execute social listening, conversation, and sentiment analysis to help measure the impact of marketing communications and identify trends/opportunities for the business.
- **Social Media – Best Practices and Processes**
  - Support social listening and escalation in partnership with consumer relations, as well as conversation and sentiment analysis to help measure the impact of marketing communications and identify trends/opportunities for the business.
  - Lead and establish social media best practices and socialize with all stakeholders.
  - Acts as the internal social media expert, share knowledge of the digital space with teams, host review meetings, and learning sessions
  - Acts as an internal social media consultant to support collaboration and expansion of activities
  - Develops community guidelines for main channels such as Facebook.
  - Develops the internal social media playbook.
  - Leads and refines community management processes at the enterprise while collaborating with cross-functional teams.
  - Focuses on ROI and KPI in the digital asset management processes

- **Social Media Campaigns**
  - Has a significant role in consulting on and executing all social media campaigns in partnership with brand management.
  - Advises on the individual campaign and total the enterprise's social media strategies to ensure all appropriate trends and tactics are considered/applied.
  - Manages social media creative development
  - Ensures prioritization and consistency between the campaign and other enterprise strategies
  - Has responsibility for making sure a systematic approach to both planning and reporting is implemented.
  - Works with the Digital Brand Manager on defining and planning the social media KPIs and ensuring these are set accurately.
  - Works with the Digital Brand Manager and agency partners to analyze cross-campaign performance to draw insights that can be applied to refine future programs.
  - Ensures assets are optimized to drive campaign objectives.
  - Supports "Always-On' paid social content is being seen by the right consumers on the right channel on the right device at the right time.
  - Ensures campaigns have appropriate social media activations that are on strategy and optimized for the social channel.
- **Digital Marketing Campaigns and Website**
  - Supports digital marketing activities as needed.
  - Supports tracking and management of ongoing updates to web content as needed.
  - Supports the troubleshooting of digital efforts as needed.
- **Innovation/Emerging Technology**
  - Helps the marketing team to innovate through influencer programs.
  - Helps the marketing team to maximize the way they use and think about data.
  - Fosters a culture of "Test and Learn" within our marketing team.
  - Identifies opportunities to try new things and evaluates effectiveness. Scale if successful, move on if not.
  - Take advantage of the enterprise's location to foster relationships with external technology companies.
  - Expands our network to provide access to new, interesting opportunities.

Authority

- The Social Media Specialist has the authority to recommend the purchase of equipment necessary for the brand management strategy (within the guidelines established by the enterprise).
- The Social Media Specialist has the authority to request external consultants as necessary to assist in all social networking strategy activities (within the guidelines established by the enterprise and IT).
- Hiring - The Social Media Specialist will hire/terminate direct reports, as well as approve staff reporting to the direct reports. Included in this responsibility is the discipline, promotion, salary adjustment, etc., of staff including providing guidelines for all technology functions within the enterprise including the SBUs that may not directly report to this position.

- Budgetary - The Social Media Specialist is responsible for oversight and review of staffing, projects, and performance of all digital strategy functions of the organization.
- Contract Review - All contracts for digital strategy are subject to a review by the Social Media Specialist.

Contacts

Internal Contacts - The most frequent internal contracts are with the Vice President Marketing, Digital Brand Manager, enterprise executive management, SBU senior management, the Chief Information Officer, and technology staff of all SBUs.

External Contacts - The primary external contacts are with contract service providers, customers, vendors, and industry peers. Contact with social media technology product and service companies is also made periodically.

Position Requirements

- Experience in Social Media Marketing and Integrated Marketing
- Excellent verbal & written communication skills – must be able to translate new digital concepts to various stakeholders, and write engaging consumer-facing content.
- Familiarity with social media analytics & measurements.
- Critical eye for design; high standards for content quality
- Collaborative, team-oriented spirit with a history of success developing cross-functional relationships & leading cross-functional projects
- Ability to plan across social media channels, then execute with discipline
- Ability to align priorities towards a forward-moving body of work centered on Business goals (Awareness, Acquisition, Conversion, etc.)
- Experience & comfort managing day-to-day communication with third-party vendors and key partners (e.g. resolve issues, document challenges, create roadmaps, facilitate collaborative brainstorming sessions, etc.)
- Strong project management skills
- Computer Experience: Basic HTML Coding, CMS tools, Adobe Creative Suite, Social Listening/Analytics Platforms, JavaScript, Salesforce/other ESP, E-commerce experience a plus
- The Social Media Specialist should have a background in business management and understand the language of financial statement analysis, ROI, KPIs, and change management.
- College degree (BA or BS); background in Marketing, Communications, Public Relations, Business, Computer Science or related field. MBA preferred.
- 2+ years of social media marketing
    - 1-2 years' experience managing multiple social media channels
    - 1-2 years' experience managing PPC campaigns
    - 1-2 years experience managing websites, coordinating web projects and email campaigns (agency experience helpful)
- Has excellent verbal and written communication skills, previous leadership,

- Has strong conceptual, analytical, judgment, and communication abilities.

Career Ladder

The Social Media Specialist can fill a senior IT position or marketing within the enterprise. Beyond this lateral movement, the logical promotional progression would be into the Brand Management position.

Social Media Specialist

Janco Associates, Inc.

Disaster Recovery – Remote Location Contact Information

Location	Main Phone Number	Facility Manager	Direct Line	Mobile	Email

Completed by: Department: Date: Click here to enter a date.

Administrative Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Information Technology Records - Computer and Information Security

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Information Technology Records - Computer Operations and Technical Support

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Information Technology Records - Data Administration

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Facility Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Financial Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Information Technology Records – IT General Systems and Application Development

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Mobile Device Access and Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

Employee agrees to adhere to the Mobile Device Access and Use Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ No
Copy of the ENTERPRISE Mobile Device Access and Use Policy and the Record Management Policy have been given to and read by the employee	☐ Yes	☐ No

Equipment/Expenses

- An employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. Enterprise equipment will be serviced and maintained by ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- The ENTERPRISE is not liable for damages to an employee's personal or real property during the performance of work duties or while using enterprise equipment in the employee's residence.
- The ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.

By signing this form, I affirm my willingness to abide by ENTERPRISE's mobile device access policies, procedures, and guidelines.

Employee Signature *Date*

Supervisor *Date*

Information Technology Records – Network and Communication Services

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Personnel Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition
PI-1	**Alcohol and Drug Abuse Program**	Records concerning alcohol and drug abuse rehabilitation program		Destroy in office after 3 years.
PI-2	**Affirmative Action and Equal Opportunity (EEO)**	Enterprise participation in federal and state affirmative action / equal opportunity programs.	correspondence, regulations, guidelines, reports, directives, recruitment plans, equal opportunity statements, full-time and part-time actions employment reviews, procedures	Original: Transfer policies, guidelines, correspondence, affirmative action plans, and compliance reviews to archives after 5 years. Destroy in office remaining records after 5 years. Reference: Destroy in office after 5 years.
PI-3	**Employment History**	A complete history of an employee's service.	forms, reports, correspondence	Transfer to appropriate individual personnel file when completed.
PI-4	**Applications for Employment**		applications resume, vitae, recommendations, correspondence, other related records	Original: Transfer applications and other records for individuals hired to appropriate personnel file when an individual accepts the position. Destroy in office applications and other records that are not solicited and for individuals not hired 3 years after the date of receipt, if no charge of discrimination has been filed. If a charge has been filed, destroy it 1 year after the resolution of the charge. Reference: Destroy in office when an employment decision is made.
PI-5	**Disciplinary Actions**	Disciplinary actions brought against employees	correspondence, forms	Original: Destroy in office 5 years after final resolution. Destruction after final resolution may occur earlier if permitted by state law. Reference: Destroy in office when reference value ends.
PI-6	**Disability Salary Continuation Claim**	Claims completed by disabled employees	applications for salary continuation, claim forms	Original: Transfer to dept handling disability claim. Reference: Transfer to the appropriate individual personnel file.

Safety Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Sales Records

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

Information Technology Records – User and Office Automation Support

This Schedule applies to records in all media unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

JANCO ASSOCIATES, INC.

Work From Home IT Checklist

Both the employee and supervisor should initial each piece of equipment in the issued box and returned box with the equipment is issued or returned.

Employee:	Department:
Location:	Supervisor:
Phone at Location:	Date:

The alternate work location is located (check one): ☐ in home ☐ not in home

Hardware Requirements		
• Base Platform (e.g. laptop, desktop with monitor, tablet)	☐YES	☐NO
• Printer	☐YES	☐NO
• Microphone / headset	☐YES	☐NO
• Camera for video conference	☐YES	☐NO
• Scanner	☐YES	☐NO
• Shredder	☐YES	☐NO
Communication Requirements		
• Landline – linked to enterprise auto attendant	☐YES	☐NO
• Internet broadband	☐YES	☐NO
• VPN	☐YES	☐NO
• Email	☐YES	☐NO
• Instant Messaging	☐YES	☐NO
• File Sharing	☐YES	☐NO
• Records retention and destruction policies	☐YES	☐NO
Security and Compliance Requirements		
• Two-factor access (password plus biometrics)	☐YES	☐NO
• Enciphering	☐YES	☐NO
• Disaster Recovery Business Continuity plan	☐YES	☐NO
• Physical Security of all electronic assets located remotely	☐YES	☐NO
• User access to admin functions blocked	☐YES	☐NO
• Media copying blocked (CD/DVD/USB connectivity)	☐YES	☐NO
• Training for telecommuter	☐YES	☐NO
Other Considerations		
• Reimbursement policy for WFH work-related expenses	☐YES	☐NO
• Policy for non-business use of enterprise assets	☐YES	☐NO
• Inventory of data and enterprise physical assets	☐YES	☐NO
• Rules for audit and termination procedures for employees	☐YES	☐NO
• Records Management procedures Implemented for WFH	☐YES	☐NO

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Work From Home IT Checklist

Both the employee and supervisor should initial each piece of equipment in the issued box and returned box with the equipment is issued or returned.

Employee:	Department:
Location:	Supervisor:
Phone at Location:	Date:

The alternate work location is located (check one): ☐ in home ☐ not in home

Hardware Requirements		
• Base Platform (e.g. laptop, desktop with monitor, tablet)	☐YES	☐NO
• Printer	☐YES	☐NO
• Microphone / headset	☐YES	☐NO
• Camera for video conference	☐YES	☐NO
• Scanner	☐YES	☐NO
• Shredder	☐YES	☐NO
Communication Requirements		
• Landline – linked to enterprise auto attendant	☐YES	☐NO
• Internet broadband	☐YES	☐NO
• VPN	☐YES	☐NO
• Email	☐YES	☐NO
• Instant Messaging	☐YES	☐NO
• File Sharing	☐YES	☐NO
• Records retention and destruction policies	☐YES	☐NO
Security and Compliance Requirements		
• Two-factor access (password plus biometrics)	☐YES	☐NO
• Enciphering	☐YES	☐NO
• Disaster Recovery Business Continuity plan	☐YES	☐NO
• Physical Security of all electronic assets located remotely	☐YES	☐NO
• User access to admin functions blocked	☐YES	☐NO
• Media copying blocked (CD/DVD/USB connectivity)	☐YES	☐NO
• Training for telecommuter	☐YES	☐NO
Other Considerations		
• Reimbursement policy for WFH work-related expenses	☐YES	☐NO
• Policy for non-business use of enterprise assets	☐YES	☐NO
• Inventory of data and enterprise physical assets	☐YES	☐NO
• Rules for audit and termination procedures for employees	☐YES	☐NO
• Records Management procedures Implemented for WFH	☐YES	☐NO

Employee Signature *Date*

Supervisor *Date*

Mobile Device Access and Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

Employee agrees to adhere to the Mobile Device Access and Use Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ No
Copy of the ENTERPRISE Mobile Device Access and Use Policy and the Record Management Policy have been given to and read by the employee	☐ Yes	☐ No

Equipment/Expenses

- An employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. Enterprise equipment will be serviced and maintained by the ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- The ENTERPRISE is not liable for damages to an employee's personal or real property during the performance of work duties or while using enterprise equipment in the employee's residence.
- The ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.

By signing this form, I affirm my willingness to abide by the ENTERPRISE's mobile device access and policies, procedures, and guidelines.

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Mobile Device Security and Compliance Checklist

Employee Name _____ ID Number _____

Job Title _____ Location _____

Device Type ☐Phone ☐Tablet ☐Other Description _____

Security Controls

Yes	No	
☐	☐	256 bit AES encryption per file at rest, a 30-day rotating encryption key
☐	☐	256 bit SSL encrypted data transfer
☐	☐	SSAE 16 Type II compliant, redundant data centers and DR policy
☐	☐	99.9% SLA Uptime Guarantee

Remote Device Management

Yes	No	
☐	☐	Auto-timed screen log out on mobile devices
☐	☐	Custom 4-digit passcode
☐	☐	Immediate access restriction on device
☐	☐	Auto-login to end-user accounts for remote wipe

Access Management Controls

Yes	No	
☐	☐	Prohibit access to App/Web UI from the admin console
☐	☐	Prohibit access to content (folders and groups) from the admin console
☐	☐	Domain Identity Control: SSO available on mobile apps

Compliance Disaster Recovery – Business Continuity

Yes	No	
☐	☐	Has the user of this device completed all of the acknowledgment and use forms
☐	☐	Is this device and all of its data backed up
☐	☐	Is this device included in the Disaster Recovery Business Continuity Plan
☐	☐	Does this device meet the compliance requirements for the record management process
☐	☐	Has the user of this device completed all necessary training

Audit Trail

Yes	No	
☐	☐	All global files can be accessed directly from the central admin console
☐	☐	Usage statistics tracked for files, individual users, and groups
☐	☐	Complies with record management policy
☐	☐	Downloads, uploads, previews
☐	☐	Tracked by IP Address

Employee Signature *Date*

Privacy Policy Compliance Acceptance Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

I hereby certify that I have reviewed ENTERPRISE's Privacy Policy Compliance and understand the policy, its standards, and procedures contained therein.

Mandated privacy requirements are designed to protect the individual's privacy from unwarranted invasion, to make sure that personal information in possession of an entity is properly used, and to prevent any potential misuse of personal information in the possession of that entity. This policy establishes the processes and procedures, and assigns responsibilities, for fulfilling mandated privacy requirements.

By signing this form, I affirm my willingness to abide by ENTERPRISE's security and sensitive information policies, procedures, and guidelines.

Signature _____ Date Click here to enter a date.

Security Access Application Form

Employee Name _____ ID Number _____
Job Title _____ Work Site _____

If your position is similar to another employee in your area or you are replacing another employee, please identify the employee:

If you need access other than the default access for your position, please indicate the additional applications or functions needed. Also, if you already have access, but feel you need additional applications or functions then indicate below:

Do you need Internet training?

☐ *No* ☐ *Yes (Intermediate)*
☐ *Yes (Novice)* ☐ *Yes (Advanced)*

Email Address

Initial Password

I hereby certify that I have reviewed the ENTERPRISE's Security Manual, and understand the restrictions and regulations contained therein. By signing this form, I affirm my willingness to abide by the ENTERPRISE's security policies, procedures, and guidelines

Signature _____ Date Click here to enter a date.

Approval Process

Dept. Head _____
☐ **Approved**
Signature _____
Comments
Date: Click here to enter a date.

IT Department _____
☐ **Approved**
User Level
☐ **Basic user**
☐ **Supervisor**
☐ **Manager**
☐ **Administrator**

Sensitive Information Policy Compliance Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

I hereby certify that I have reviewed ENTERPRISE's Secure Information policy and understand the policy, its standards, and procedures contained therein.

Sensitive and confidential information is defined as information that is protected against unwarranted disclosure. Access to sensitive information is to be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues about personal privacy, or proprietary considerations.

Information sensitivity is the control of access to information or knowledge that might result in the loss of an advantage or level of security if disclosed to others.

Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business, or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information. I understated that if I violate this policy, its standards, or procedures, I am subject to immediate termination without recourse.

By signing this form, I affirm my willingness to abide by ENTERPRISE's security and sensitive information policies, procedures, and guidelines.

Signature _____ Date Click here to enter a date.

JANCO ASSOCIATES, INC.

Server Registration

Server ID	Server Name	Location	Type Location	Server Admin	Contact Number	Data Type(s)	Application(s)	Services
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL
			☐Data Center ☐Office ☐Cloud			☐Sensitive ☐Confidential ☐Public		☐Web ☐FTP ☐SSL

Completed by:

Department:

Date: Click here to enter a date.

JANCO ASSOCIATES, INC.

Telecommuting Work Agreement

The following constitutes an agreement on the terms and conditions of telecommuting on (Date) between:

Employee Signature *Date*

Supervisor *Date*

Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.	☐YES	☐NO
Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____. This agreement may be extended beyond the initial one year period, if agreeable to the ENTERPRISE and the employee. If extended, the terms of this agreement should be reviewed and updated as necessary. This agreement can be terminated at any time by ENTERPRISE without notice.	☐YES	☐NO
ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.	☐YES	☐NO
Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.	☐YES	☐NO

Work Location – Schedule

Employee's central workplace is:

Employee's Work From Home location is

Describe in detail the designated work area at the WFH location.

At the central workplace, employee's work hours will normally be from to

on the following days:

At the WFH location, employee's work hours will normally be from to

on the following days:

Employee's time and attendance will be recorded the same as performing official duties at the central workplace.

Supervisors will maintain a copy of the employee's work schedule, and the employee's time and attendance will be recorded the same as if performing official duties at the central workplace.

Approval Process

Dept. Head _____ ☐ **Approved**

Signature _____

Comments

Date:

IT Department _____

User Level

☐ **Approved**

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

Work Standards/Performance

- Employees will meet with the supervisor to receive assignments and to review completed work as necessary or appropriate.
- The employee will complete all assigned work according to work procedures mutually agreed upon by the employee and the supervisor, and according to guidelines and expectations stated in the employee's performance plan.
- The supervisor will evaluate an employee's job performance according to the employee's performance plan.
- Employee agrees to limit the performance of his/her officially-assigned duties to the central workplace or ENTERPRISE-approved alternate work location. Failure to comply with this provision may result in loss of pay, termination of the telecommuting agreement, and/or appropriate disciplinary action.

Compensation/Benefits

- All salary rates, leave accrual rates, and travel entitlements will remain as if the employee performed all work at the central workplace.
- The employee will be compensated following applicable law and state policy for overtime work that has been requested by his/her supervisor and approved in advance.
- Employee understands that overtime work must be approved in advance by the supervisor. By signing this form, the employee agrees that failing to obtain proper approval for overtime work may result in his/her removal from telecommuting and/or termination and/or appropriate action.
- Employees must obtain supervisory approval before taking leave following established office procedures. By signing this form, the employee agrees to follow established procedures for requesting and obtaining approval of leave.

Equipment/Expenses

- The employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. State-owned equipment will be serviced and maintained by the ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- Neither the ENTERPRISE nor the state will be liable for damages to an employee's personal or real property during the performance of official duties or while using state equipment in the employee's residence.
- Neither the ENTERPRISE nor the state will be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Safety

- The employee is covered by the appropriate provisions of the State's Workers' Compensation Program or the ENTERPRISE Sickness and Disability Program, as appropriate, if injured while performing official duties at the central workplace or alternate work location.
- Employee agrees to certify that the work location is safe and free from hazards.
- Employee agrees to bring to the immediate attention of his/her supervisor any accident or injury occurring at the alternate work location while working.
- A supervisor will investigate all accident and injury reports immediately following notification.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.
- The employee will comply with ENTERPRISE record management, retention, and disposition policy.

Initiation and Termination of Agreement

- This agreement is NOT a guarantee of employment
- Employee agrees to adhere to applicable guidelines and policies.
- ENTERPRISE concurs with employee participation and agrees to adhere to applicable policies and procedures.
- The employee may terminate participation in telecommuting at any time unless it was a condition of employment. One (1) week may be provided before the termination of his agreement.
- ENTERPRISE may terminate an employee's participation in telecommuting at any time. (Employees may be withdrawn for reasons to include, but not limited to, declining performance and organizational benefit). One (1) week may be provided before the termination of his agreement.

Text Messaging Sensitive Information Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

Employee agrees to adhere to the Text Messaging Sensitive and Confidential Information Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee need to text message sensitive and/or confidential information	☐ Yes	☐ No
Copies of the ENTERPRISE Text Messaging Sensitive and Confidential Information and Record Management Policy have been given to and read by the employee	☐ Yes	☐ No

Confidentiality/Security

- An employee who texts messages ENTERPRISE's sensitive and/or confidential information agrees to protect such information following ENTERPRISE guidelines. Such information remains the property of the ENTERPRISE.
- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.

Equipment/Expenses

- If the employee provides equipment, he/she is responsible for servicing and maintaining that equipment and text messaging application conforms to the ENTERPRISE's text Messaging Sensitive and Confidential Information Policy.
- The ENTERPRISE is not liable for damages to an employee's personal or real property during the performance of work duties or while using enterprise equipment in the employee's residence.
- The ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

By signing this form, I affirm my willingness to abide by the ENTERPRISE's Text Messaging Sensitive and Confidential Information Policy.

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Work From Home Work Agreement

The following constitutes an agreement on the terms and conditions of telecommuting on (Date) between:

Employee Signature *Date*

Supervisor *Date*

Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.	☐YES	☐NO
Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____. This agreement may be extended beyond the initial one year period, if agreeable to the ENTERPRISE and the employee. If extended, the terms of this agreement should be reviewed and updated as necessary. This agreement can be terminated at any time by ENTERPRISE without notice.	☐YES	☐NO
ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.	☐YES	☐NO
Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.	☐YES	☐NO

Work Location – Schedule

Employee's central workplace is:

Employee's Work From Home location is

Describe in detail the designated work area at the WFH location.

At the central workplace, employee's work hours will normally be from to

on the following days:

At the WFH location, employee's work hours will normally be from to

on the following days:

Employee's time and attendance will be recorded the same as performing official duties at the central workplace.

Supervisors will maintain a copy of the employee's work schedule, and the employee's time and attendance will be recorded the same as if performing official duties at the central workplace.

Approval Process

Dept. Head _____ ☐ **Approved**

Signature _____

Comments

Date:

IT Department _____

☐ **Approved**

User Level

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

Work Standards/Performance

- Employees will meet with the supervisor to receive assignments and to review completed work as necessary or appropriate.
- The employee will complete all assigned work according to work procedures mutually agreed upon by the employee and the supervisor, and according to guidelines and expectations stated in the employee's performance plan.
- The supervisor will evaluate an employee's job performance according to the employee's performance plan.
- Employee agrees to limit the performance of his/her officially-assigned duties to the central workplace or ENTERPRISE-approved alternate work location. Failure to comply with this provision may result in loss of pay, termination of the telecommuting agreement, and/or appropriate disciplinary action.

Compensation/Benefits

- All salary rates, leave accrual rates, and travel entitlements will remain as if the employee performed all work at the central workplace.
- The employee will be compensated following applicable law and state policy for overtime work that has been requested by his/her supervisor and approved in advance.
- Employee understands that overtime work must be approved in advance by the supervisor. By signing this form, the employee agrees that failing to obtain proper approval for overtime work may result in his/her removal from telecommuting and/or termination and/or appropriate action.
- Employees must obtain supervisory approval before taking leave following established office procedures. By signing this form, the employee agrees to follow established procedures for requesting and obtaining approval of leave.

Equipment/Expenses

- The employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. State-owned equipment will be serviced and maintained by the ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- Neither the ENTERPRISE nor the state will be liable for damages to an employee's personal or real property during the performance of official duties or while using state equipment in the employee's residence.
- Neither the ENTERPRISE nor the state will be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Safety

- The employee is covered by the appropriate provisions of the State's Workers' Compensation Program or the ENTERPRISE Sickness and Disability Program, as appropriate, if injured while performing official duties at the central workplace or alternate work location.
- Employee agrees to certify that the work location is safe and free from hazards.
- Employee agrees to bring to the immediate attention of his/her supervisor any accident or injury occurring at the alternate work location while working.
- A supervisor will investigate all accident and injury reports immediately following notification.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.
- The employee will comply with ENTERPRISE record management, retention, and disposition policy.

Initiation and Termination of Agreement

- This agreement is NOT a guarantee of employment
- Employee agrees to adhere to applicable guidelines and policies.
- ENTERPRISE concurs with employee participation and agrees to adhere to applicable policies and procedures.
- The employee may terminate participation in telecommuting at any time unless it was a condition of employment. One (1) week may be provided before the termination of his agreement.
- ENTERPRISE may terminate an employee's participation in telecommuting at any time. (Employees may be withdrawn for reasons to include, but not limited to, declining performance and organizational benefit). One (1) week may be provided before the termination of his agreement.

BYOD Access and Use Agreement

Employee Name		ID Number	
Job Title		Location	
Device Type	☐ Phone ☐ Tablet ☐ Other	Description	

Employee agrees to adhere to the BYOD and Mobile Device Access and Use Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ No
Copies of the ENTERPRISE BYOD and Mobile Device Access and Use Policy and the Record Management and Disposition policy have been given to and read by the employee	☐ Yes	☐ No

Equipment/Expenses

- Employee agrees to protect such equipment per ENTERPRISE guidelines.
- Employee agrees to comply with the record management retention and disposal policy.
- The employee is responsible for servicing and maintaining personal equipment.
- ENTERPRISE is not liable for damages to an employee's personal or real property during the performance of work-related duties or while using equipment in the employee's residence.
- ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.
- ENTERPRISE will compensate the employee for any incremental costs associated with connectivity and upgrade of equipment to support the BYOD's use on ENTERPRISE network or applications.

Confidentiality/Security/Backup

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure
- ENTERPRISE has the right to remotely wipe the contents of the device
- A PIN of at least 4 characters or numbers (or biometric scan i.e. fingerprint) will be utilized by the Employee and after 10 consecutive failed attempts ENTERPRISE has the right to automatically wipe the device
- All backups of the device will be to ENTERPRISE's network and remain the property of ENTERPRISE

By signing this form, I affirm my willingness to abide by the ENTERPRISE's BYOD access policies, procedures, and guidelines.

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Company Asset Employee Control Log

Employee Name _____ ID Number _____
Job Title _____ Location _____

Equipment	Model - Serial Number	Issued Initial	Date	Returned Initial	Date
Laptop Computer					
Modem Router					
Mobile Phone					
Printer					
Scanner					
Monitor					
Docking Station					
Tablet					
Laptop					
Desktop					

Signature _____ Date _____

Internet & Electronic Communication - Employee Acknowledgment

If you have questions or concerns about this Policy, contact the ENTERPRISE's CIO before signing this agreement[1].

I have read the ENTERPRISE's electronic communication and Internet Usage Policy and agree to abide by it. I understand the violation of any of the above terms may result in discipline, up to and including my termination.

Employee Name _____ ID Number _____

Job Title _____ Location _____

Do you need internet or computer training?

- ☐ No
- ☐ Yes (Novice)
- ☐ Yes (Intermediate)
- ☐ Yes (Advanced)

Signature _____ Date Click here to enter a date.

Approval Process

Supervisor _____

☐ **Approved**

User ID _____

Comments

IT Department _____

☐ **Approved**

Security Level

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **System Administrator**

[1] Please retain one copy of this policy with your signature with your records and forward a copy of the signed page to the office of the CIO.

Social Networking Policy Compliance Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

I hereby certify that I have reviewed ENTERPRISE's Blog Policy and understand the policy, its standards, and procedures contained therein.

- I hereby certify that I have reviewed the ENTERPRISE's Social Net policy and understand the policy, its standards, and procedures contained therein.
- I understated that if I violate this policy, its standards, or procedures, I am subject to immediate termination without recourse.
- By signing this form, I affirm my willingness to abide by ENTERPRISE's security policies, procedures, and guidelines.

By signing this form, I affirm my willingness to abide by the ENTERPRISE's Social Networking policies, procedures, and guidelines.

Signature _____ Date _____

JANCO ASSOCIATES, INC.

Telecommuting IT Checklist

Both the employee and supervisor should initial each piece of equipment in the issued box and returned box with the equipment is issued or returned.

Employee:	Department:
Location:	Supervisor:
Phone at Location:	Date:

The alternate work location is located (check one): ☐ in home ☐ not in home

Hardware Requirements		
• Base Platform (e.g. laptop, desktop with monitor, tablet)	☐YES	☐NO
• Printer	☐YES	☐NO
• Microphone / headset	☐YES	☐NO
• Camera for video conference	☐YES	☐NO
• Scanner	☐YES	☐NO
• Shredder	☐YES	☐NO
Communication Requirements		
• Landline – linked to enterprise auto attendant	☐YES	☐NO
• Internet broadband	☐YES	☐NO
• VPN	☐YES	☐NO
• Email	☐YES	☐NO
• Instant Messaging	☐YES	☐NO
• File Sharing	☐YES	☐NO
• Records retention and destruction policies	☐YES	☐NO
Security and Compliance Requirements		
• Two-factor access (password plus biometrics)	☐YES	☐NO
• Enciphering	☐YES	☐NO
• Disaster Recovery Business Continuity plan	☐YES	☐NO
• Physical Security of all electronic assets located remotely	☐YES	☐NO
• User access to admin functions blocked	☐YES	☐NO
• Media copying blocked (CD/DVD/USB connectivity)	☐YES	☐NO
• Training for telecommuter	☐YES	☐NO
Other Considerations		
• Reimbursement policy for telecommuters work-related expenses	☐YES	☐NO
• Policy for non-business use of enterprise assets	☐YES	☐NO
• Inventory of data and enterprise physical assets	☐YES	☐NO
• Rules for audit and termination procedures for employees	☐YES	☐NO

Employee Signature *Date*

Supervisor *Date*

Telecommuting Work Agreement

The following constitutes an agreement on the terms and conditions of telecommuting on (Date) between:

Employee Signature *Date*

Supervisor *Date*

Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.	☐YES	☐NO
Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____. This agreement may be extended beyond the initial one year period, if agreeable to the ENTERPRISE and the employee. If extended, the terms of this agreement should be reviewed and updated as necessary. This agreement can be terminated at any time by ENTERPRISE without notice.	☐YES	☐NO
ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.	☐YES	☐NO
Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.	☐YES	☐NO

Work Location – Schedule

Employee's central workplace is:

Employee's Work From Home location is

Describe in detail the designated work area at the WFH location.

At the central workplace, employee's work hours will normally be from to

on the following days:

At the WFH location, employee's work hours will normally be from to

on the following days:

Employee's time and attendance will be recorded the same as performing official duties at the central workplace.

Supervisors will maintain a copy of the employee's work schedule, and the employee's time and attendance will be recorded the same as if performing official duties at the central workplace.

Approval Process

Dept. Head _____ ☐ **Approved**

Signature _____

Comments

Date:

IT Department _____

☐ **Approved**

User Level

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

Work Standards/Performance

- Employees will meet with the supervisor to receive assignments and to review completed work as necessary or appropriate.
- The employee will complete all assigned work according to work procedures mutually agreed upon by the employee and the supervisor, and according to guidelines and expectations stated in the employee's performance plan.
- The supervisor will evaluate an employee's job performance according to the employee's performance plan.
- Employee agrees to limit the performance of his/her officially-assigned duties to the central workplace or ENTERPRISE-approved alternate work location. Failure to comply with this provision may result in loss of pay, termination of the telecommuting agreement, and/or appropriate disciplinary action.

Compensation/Benefits

- All salary rates, leave accrual rates, and travel entitlements will remain as if the employee performed all work at the central workplace.
- The employee will be compensated following applicable law and state policy for overtime work that has been requested by his/her supervisor and approved in advance.
- Employee understands that overtime work must be approved in advance by the supervisor. By signing this form, the employee agrees that failing to obtain proper approval for overtime work may result in his/her removal from telecommuting and/or termination and/or appropriate action.
- Employees must obtain supervisory approval before taking leave following established office procedures. By signing this form, the employee agrees to follow established procedures for requesting and obtaining approval of leave.

Equipment/Expenses

- The employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. State-owned equipment will be serviced and maintained by the ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- Neither the ENTERPRISE nor the state will be liable for damages to an employee's personal or real property during the performance of official duties or while using state equipment in the employee's residence.
- Neither the ENTERPRISE nor the state will be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Safety

- The employee is covered by the appropriate provisions of the State's Workers' Compensation Program or the ENTERPRISE Sickness and Disability Program, as appropriate, if injured while performing official duties at the central workplace or alternate work location.
- Employee agrees to certify that the work location is safe and free from hazards.
- Employee agrees to bring to the immediate attention of his/her supervisor any accident or injury occurring at the alternate work location while working.
- A supervisor will investigate all accident and injury reports immediately following notification.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.
- The employee will comply with ENTERPRISE record management, retention, and disposition policy.

Initiation and Termination of Agreement

- This agreement is NOT a guarantee of employment
- Employee agrees to adhere to applicable guidelines and policies.
- ENTERPRISE concurs with employee participation and agrees to adhere to applicable policies and procedures.
- The employee may terminate participation in telecommuting at any time unless it was a condition of employment. One (1) week may be provided before the termination of his agreement.
- ENTERPRISE may terminate an employee's participation in telecommuting at any time. (Employees may be withdrawn for reasons to include, but not limited to, declining performance and organizational benefit). One (1) week may be provided before the termination of his agreement.

Wearable Device Access and Use Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

Employee agrees to adhere to the Google Glass and Mobile Device Access and Use Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ No
Copies of the ENTERPRISE Google Glass, Mobile Device Access and Use, and Record Management Policy have been given to and been read by the employee	☐ Yes	☐ No

Equipment/Expenses

- Employee agrees to protect such equipment following ENTERPRISE guidelines.
- The employee is responsible for servicing and maintaining their equipment.
- ENTERPRISE is not liable for damages to an employee's personal or real property during the performance of work-related duties or while using equipment in the employee's residence.
- ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.
- ENTERPRISE will compensate the employee for any incremental costs associated with connectivity and upgrade of equipment to support Google Glasses' use on the ENTERPRISE network or applications.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.
- The employee will respect the privacy of all employees, associates, suppliers, customers, and others they encounter while using or wearing Google Glass.

By signing this form, I affirm my willingness to abide by ENTERPRISE's Google Glass access policies, procedures, and guidelines.

_____

Employee Signature *Date*

_____

Supervisor *Date*

JANCO ASSOCIATES, INC.

Work From Home Contact Information

Employee Name	Office Number	Manager Number	Mobile Number	Land Line	Email

Completed by: Department: Date: Click here to enter a date.

JANCO ASSOCIATES, INC.

Work From Home IT Checklist

Both the employee and supervisor should initial each piece of equipment in the issued box and returned box with the equipment is issued or returned.

Employee:	Department:
Location:	Supervisor:
Phone at Location:	Date:

The alternate work location is located (check one): ☐ in home ☐ not in home

Hardware Requirements		
• Base Platform (e.g. laptop, desktop with monitor, tablet)	☐YES	☐NO
• Printer	☐YES	☐NO
• Microphone / headset	☐YES	☐NO
• Camera for video conference	☐YES	☐NO
• Scanner	☐YES	☐NO
• Shredder	☐YES	☐NO
Communication Requirements		
• Landline – linked to enterprise auto attendant	☐YES	☐NO
• Internet broadband	☐YES	☐NO
• VPN	☐YES	☐NO
• Email	☐YES	☐NO
• Instant Messaging	☐YES	☐NO
• File Sharing	☐YES	☐NO
• Records retention and destruction policies	☐YES	☐NO
Security and Compliance Requirements		
• Two-factor access (password plus biometrics)	☐YES	☐NO
• Enciphering	☐YES	☐NO
• Disaster Recovery Business Continuity plan	☐YES	☐NO
• Physical Security of all electronic assets located remotely	☐YES	☐NO
• User access to admin functions blocked	☐YES	☐NO
• Media copying blocked (CD/DVD/USB connectivity)	☐YES	☐NO
• Training for telecommuter	☐YES	☐NO
Other Considerations		
• Reimbursement policy for WFH work-related expenses	☐YES	☐NO
• Policy for non-business use of enterprise assets	☐YES	☐NO
• Inventory of data and enterprise physical assets	☐YES	☐NO
• Rules for audit and termination procedures for employees	☐YES	☐NO
• Records Management procedures Implemented for WFH	☐YES	☐NO

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Work From Home Work Agreement

The following constitutes an agreement on the terms and conditions of telecommuting on (Date) between:

Employee Signature *Date*

Supervisor *Date*

Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.	☐YES	☐NO
Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____. This agreement may be extended beyond the initial one-year period, if agreeable to the ENTERPRISE and the employee. If extended, the terms of this agreement should be reviewed and updated as necessary. This agreement can be terminated at any time by ENTERPRISE without notice.	☐YES	☐NO
ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.	☐YES	☐NO
Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.	☐YES	☐NO

Work Location – Schedule

Employee's central workplace is:

Employee's Work From Home location is

Describe in detail the designated work area at the WFH location.

At the central workplace, employee's work hours will normally be from to

on the following days:

At the WFH location, employee's work hours will normally be from to

on the following days:

Employee's time and attendance will be recorded the same as performing official duties at the central workplace.

Supervisors will maintain a copy of the employee's work schedule, and the employee's time and attendance will be recorded the same as if performing official duties at the central workplace.

Approval Process

Dept. Head _____ ☐ **Approved**

Signature _____

Comments

Date:

IT Department _____

User Level

☐ **Approved**

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

Work Standards/Performance

- Employees will meet with the supervisor to receive assignments and to review completed work as necessary or appropriate.
- The employee will complete all assigned work according to work procedures mutually agreed upon by the employee and the supervisor, and according to guidelines and expectations stated in the employee's performance plan.
- The supervisor will evaluate an employee's job performance according to the employee's performance plan.
- Employee agrees to limit the performance of his/her officially-assigned duties to the central workplace or ENTERPRISE-approved alternate work location. Failure to comply with this provision may result in loss of pay, termination of the telecommuting agreement, and/or appropriate disciplinary action.

Compensation/Benefits

- All salary rates, leave accrual rates, and travel entitlements will remain as if the employee performed all work at the central workplace.
- The employee will be compensated following applicable law and state policy for overtime work that has been requested by his/her supervisor and approved in advance.
- Employee understands that overtime work must be approved in advance by the supervisor. By signing this form, the employee agrees that failing to obtain proper approval for overtime work may result in his/her removal from telecommuting and/or termination and/or appropriate action.
- Employees must obtain supervisory approval before taking leave following established office procedures. By signing this form, the employee agrees to follow established procedures for requesting and obtaining approval of leave.

Equipment/Expenses

- The employee who uses ENTERPRISE equipment agrees to protect such equipment following ENTERPRISE guidelines. State-owned equipment will be serviced and maintained by the ENTERPRISE.
- If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- Neither the ENTERPRISE nor the state will be liable for damages to an employee's personal or real property during the performance of official duties or while using state equipment in the employee's residence.
- Neither the ENTERPRISE nor the state will be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee's residence as an alternate work location.

Safety

- The employee is covered by the appropriate provisions of the State's Workers' Compensation Program or the ENTERPRISE Sickness and Disability Program, as appropriate, if injured while performing official duties at the central workplace or alternate work location.
- Employee agrees to certify that the work location is safe and free from hazards.
- Employee agrees to bring to the immediate attention of his/her supervisor any accident or injury occurring at the alternate work location while working.
- A supervisor will investigate all accident and injury reports immediately following notification.

Confidentiality/Security

- The employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements outlined in the ENTERPRISE policy or procedure.
- The employee will comply with ENTERPRISE record management, retention, and disposition policy.

Initiation and Termination of Agreement

- This agreement is NOT a guarantee of employment
- Employee agrees to adhere to applicable guidelines and policies.
- ENTERPRISE concurs with employee participation and agrees to adhere to applicable policies and procedures.
- The employee may terminate participation in telecommuting at any time unless it was a condition of employment. One (1) week may be provided before the termination of his agreement.
- ENTERPRISE may terminate an employee's participation in telecommuting at any time. (Employees may be withdrawn for reasons to include, but not limited to, declining performance and organizational benefit). One (1) week may be provided before the termination of his agreement.