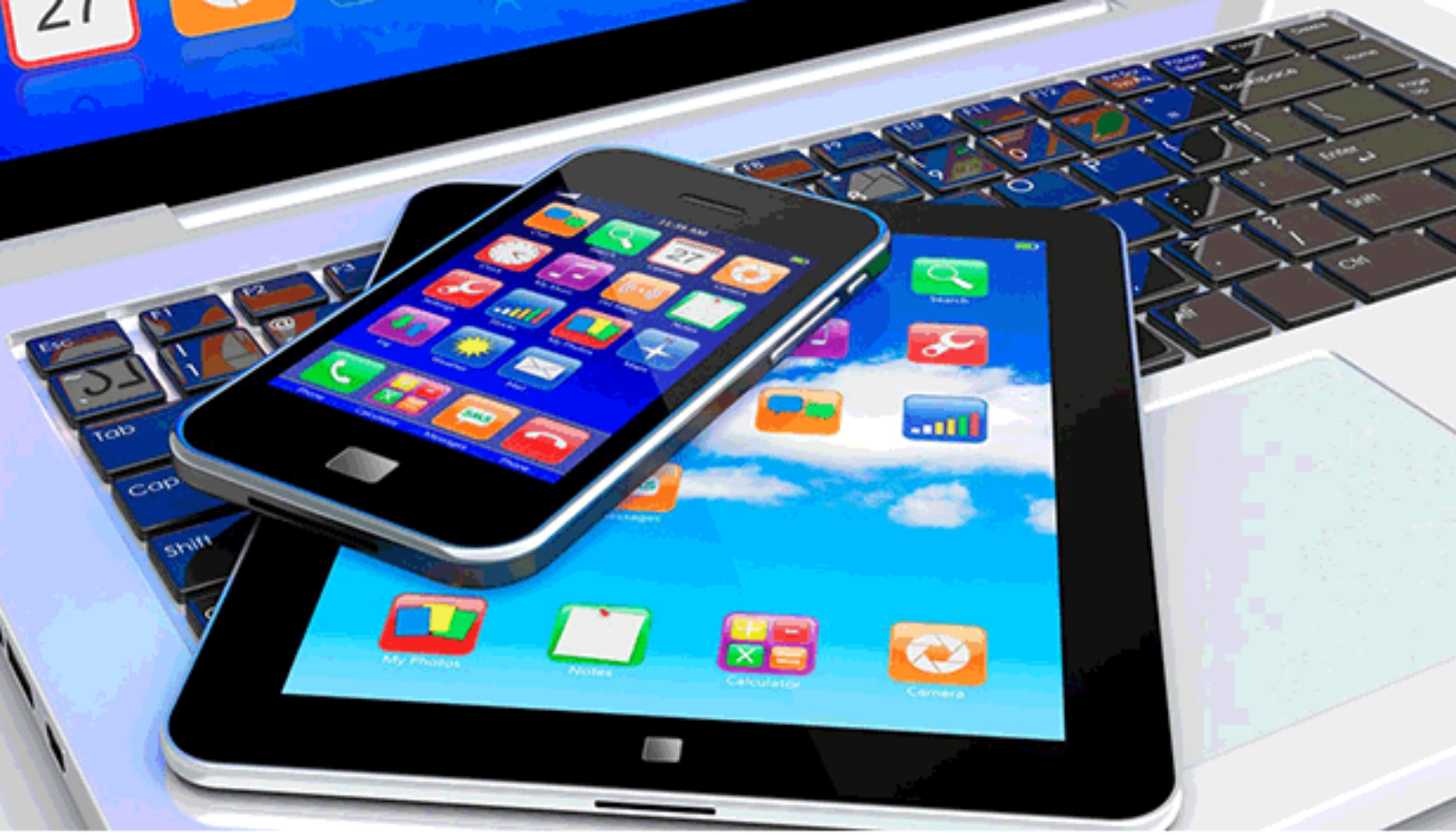


WFH & Mobility Infrastructure Policy Bundle

2024

Janco Associates, Inc.

Contents

Work From Home & Mobiliy Infrastrcture Policy Bundle

- Overview
- Policies
- Job Descriptions
- Electronic forms

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

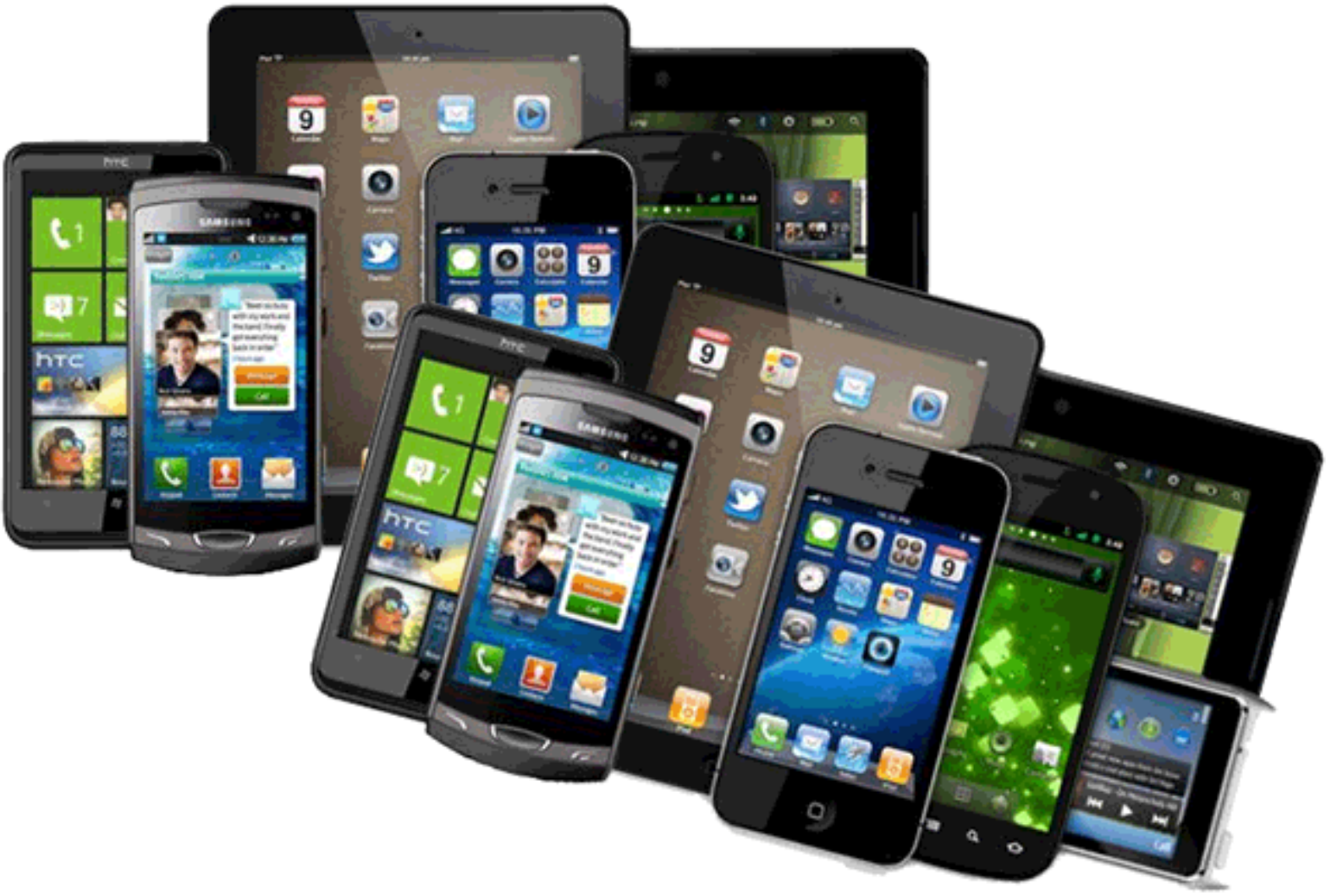
In addition, along with the 8 policies, included are electronic forms and full job descriptions to assist in the administration and management of the mobile workforce.

Job Descriptions

- Chief Compliance
- 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
- 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
- Others
  - 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



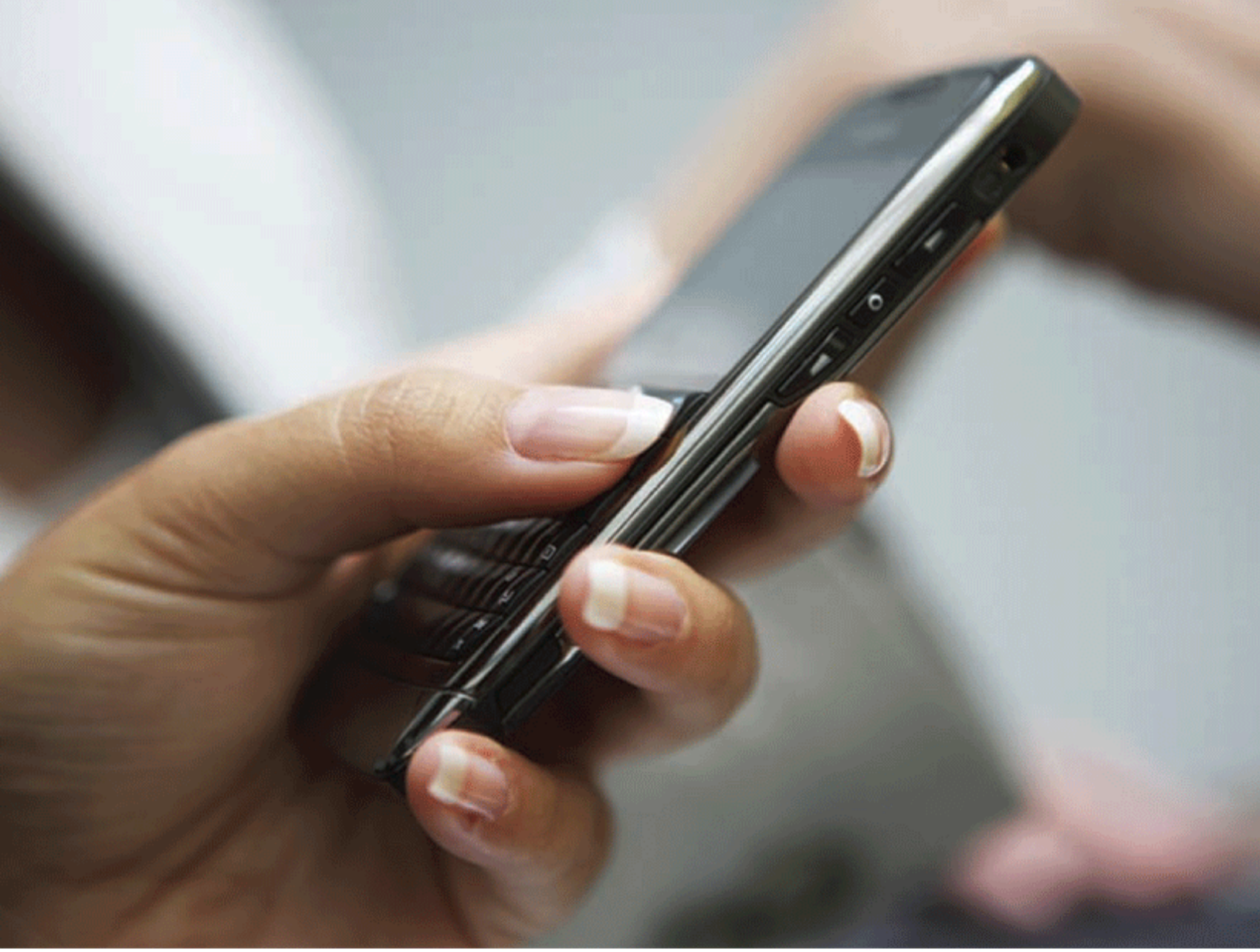
BYOD Policy Template

Janco Associates, Inc.

2024

Table of Contents

Bring Your Own Device (BYOD) Access and Use Policy 3
Overview 3
Components of the BYOD Strategy and Basics for BYOD Policy 4
Device Ownership Issues 7
Policy 8
Device Requirements 8
Policy Definitions 9
Access Control 9
Security 10
Help & Support 11
Enterprise Mobile Device Infrastructure 11
BYOD Infrastructure 12
Disaster Recovery 12
Termination 12
Backups 12
Tablet Computer (iPads) 13
Internal Network Access 13
Repair Procedure 13
Upgrade Procedure 13
Patching Policy 13
BYOD Security Best Practices 14
Work From Home - Best Practices 16
BYOD Metrics and SLA Agreement 17
Legal Considerations 19
Appendix 22
BYOD Policy Decision Table 23
Electronic Forms 24
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 25
BYOD Support Specialist
BYOD Support Supervisor
Manager BYOD Support
Manager WFH Support
What's New 26



Mobile Device Access & Use Policy

Janco Associates, Inc.

2024

Table of Contents

Mobile Access and Use Policy 2

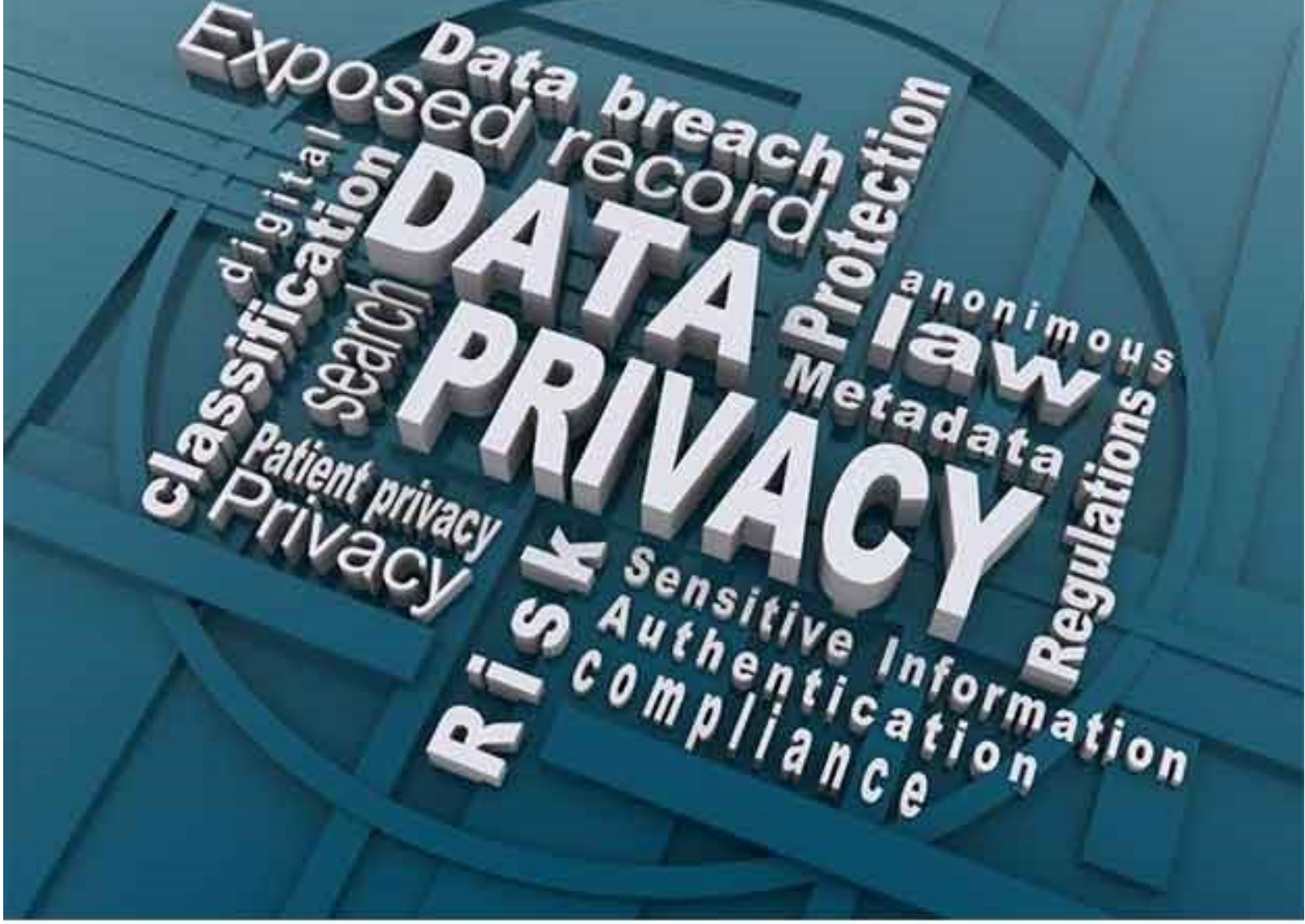
Overview 2
Components of the BYOD Strategy and Basics for BYOD Policy 3

Policy 6
Policy and Appropriate Use 6
Mobile Devices 8
Policy Definitions 9
Access Control 9
Federal Trade Commission Mobile Policy Guidelines 10
Security 11
Help & Support 12
Enterprise Mobile Device Infrastructure 13
Equipment and Supplies 13
Tablet Computer (iPads and Microsoft Surface) 14

Mobile Device Security Best Practices 16
Mobile Device Security Best practices 16
Security controls 16
Remote device management 17
Access management controls 17
Tablet and Smartphone applications 17

Appendix 18
Electronic Forms 19
- 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 20



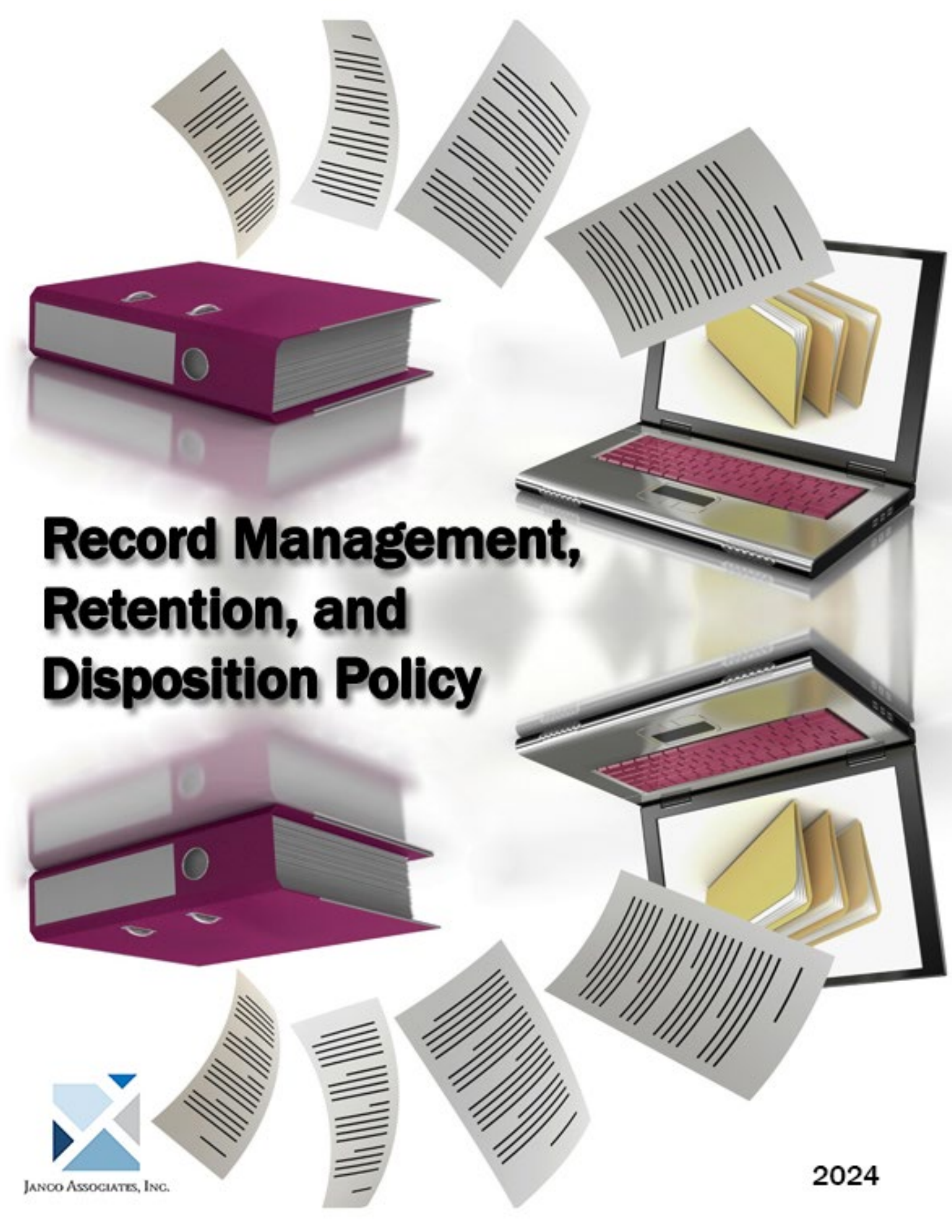
Privacy Compliance Policy

Jango Associates

2024

Table of Contents

Privacy Compliance Policy – U.S. and EU Mandated Requirements....3
Overview....3
Right to Privacy....3
California Consumer Privacy Act of 2018....4
Consumer's Right to Know Information that Has Been Captured....4
Consumer's Right to Have Data Removed....5
Consumer's Right to Know How Data is Used....6
Consumer's Rights to Data That is Sold....7
Consumer's Rights for Stopping the Sale of Data....8
Consumer's Rights to Not be Discriminated Due to Opt Out....9
Enterprise Reporting Requirements....10
Enterprise Internet and WWW requirements....12
GDPR....13
Why Data is Captured....13
User Consent....14
Communication....15
Third Party Data....15
Profiling....16
Legacy data....16
PCI....17
HIPAA....20
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999....21
Massachusetts 201 CMR 17.00 Data Protection Requirements....22
User/Customer Sensitive Information and Privacy Bill of Rights....23
Appendix....24
Forms....24
Privacy Compliance Policy Acceptance Agreement
Job Descriptions....25
Chief Security Officer
Data Protection Officer
Manager Compliance
Manager Security and Workstations
Security Architect
Privacy and Security Compliance Implementation Work Plan....26
What's New....28



Record Management, Retention, and Disposition Policy

Janco Associates, Inc.

2024

Table of Contents

Record Classification, Management, Retention, and Disposition Policy Statement 2
Overview 2
Scope 3
Work From Home impact 3
AI impact 3
What is Record Classification and Management 4
Regulatory Overview 5
What ENTERPRISE Should Do 10
Record Classification, Management, Retention, and Disposition Standard 11
Email Retention Compliance 25
Implementation Interview Checklist 30
Record classification, management, retention, and disposition Annual Review Process 31
Record Management Best Practices 33
Appendix 37
Job Descriptions 38
Manager – Record Administrator
Manager WFH Support
Record Management Coordinator
Forms 39
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 39
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 40
Federal Law Record Retention 41
Pennsylvania Record Retention 50
Massachusetts Record Retention 53
I-9 Retention 55
Version History 58

Social Networking Policy

Managing and Controlling Employee Social Networks

Janco Associates, Inc.

2024

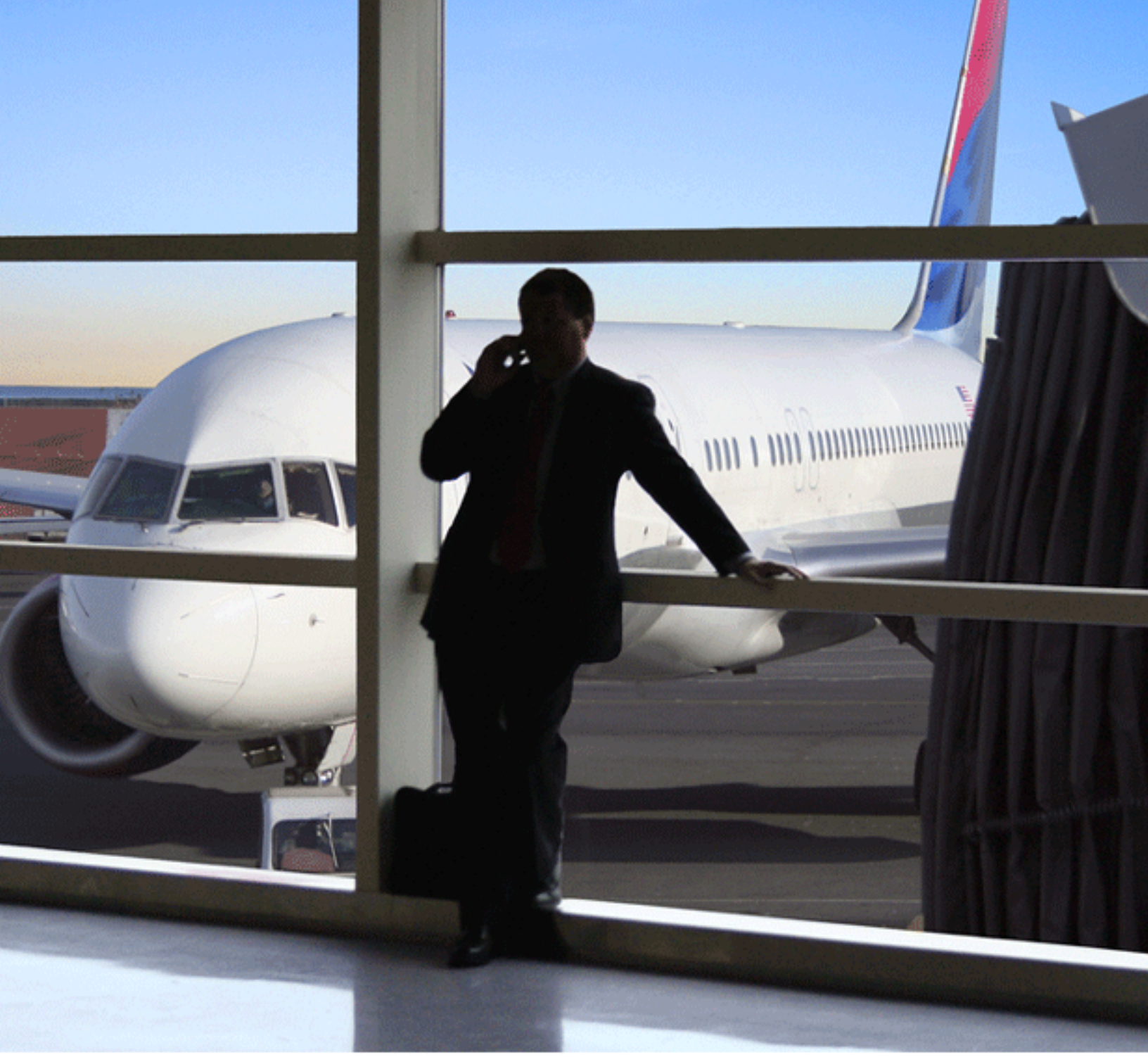
Table of Contents

Policy – Social Networking 3
Definitions 3
Overview 3
Rights to content 8
Rules for Social Network Engagement 11
Social Network Best Practices and Guidelines 13
Security Standards 16
BYOD Security 17
Protect Sensitive Data 17
Disaster Recovery and Business Continuity 18
Best Practices in Managing Social Networks and Social Relationships 19
Steps to Prevent Being Scammed by Social Media 20

Appendix 21
Job Descriptions 22
- Chief Experience Officer
- Manager Social Networking
- Social Media Specialist

Electronic Forms 23
- Internet and Electronic Communication Agreement
- Social Network Policy Compliance Agreement

Protection from Ransomware, Phishing, and Whaling Attacks 24
Social Networking Best Practices 28
Twitter 28
Truth Social 30
LinkedIn 31
Blog 33
What's New 36



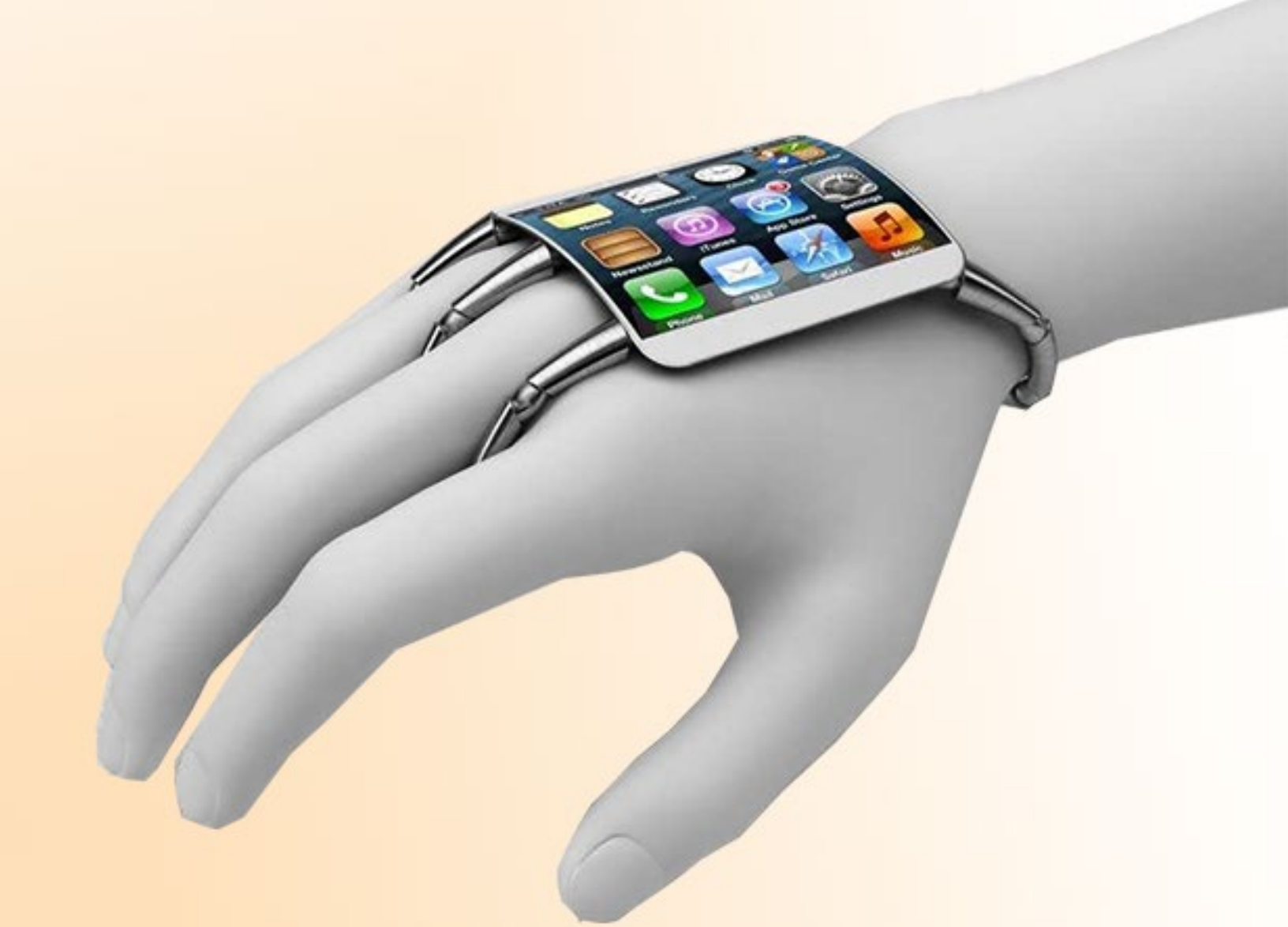
Travel, Laptop, PDA, and Off-Site Meeting Policy

2024

Jancoo Associates, Inc.

Table of Contents

Travel, Laptop, PDA, and Off-Site Meetings 3
Laptop and PDA Security 3
BYOD Security 3
Service Provider Selection 4
Wi-Fi & VPN 4
Data and Application Security 5
Minimize Attention 5
Public Shared Resources – Wireless and Shared Computers 6
Off-Site Meeting Special Considerations 7
Pandemic Issues 8
International Travel Best Practices 8
Remote Computing Best Practices 9
Electronic Meetings 11
Best Practices for Electronic Meetings 12
Appendix 13
Job Description 14
Chief Experience Officer
Chief Mobility Officer
Manager Help Desk Support
Manager Telecommuting
Manager WFH Support
Electronic Forms 15
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 16



Wearable Device Policy

2024

Janco Associates, Inc.

Table of Contents

Wearable Device Policy 3
- Overview 3
- Policy 3
- Creating a Wear Your Own Device Strategy (WYOD) 7
- Enterprise Mobile Device Infrastructure 8
  - Wearable Device Infrastructure 8
  - Disaster Recovery 8
  - Backups 9
  - Wearable Device Physical Device 9
  - Internal Network Access 9
  - Repair Procedure 10
  - Upgrade Procedure 10
  - Patching Policy 10
  - Ownership of device 10
  - Ownership of data 10
- Wearable Devices Security Best Practices 12
  - Security Controls 12
  - Remote Wearable Devices Management 12
  - Access Management Controls 13
  - Wearable Device Applications 13
- Legal Considerations 14
  - Privacy 14
  - Record Retention 15
- WYOD Management Security Options 17
- Appendix 18
  - Top 10 WYOD Best Practices 19
  - Electronic Forms 20
    - Mobile Device Access and Use Agreement
    - Mobile Device Security and Compliance Checklist
    - Wearable Device Access and Use Agreement
  - What's New 21

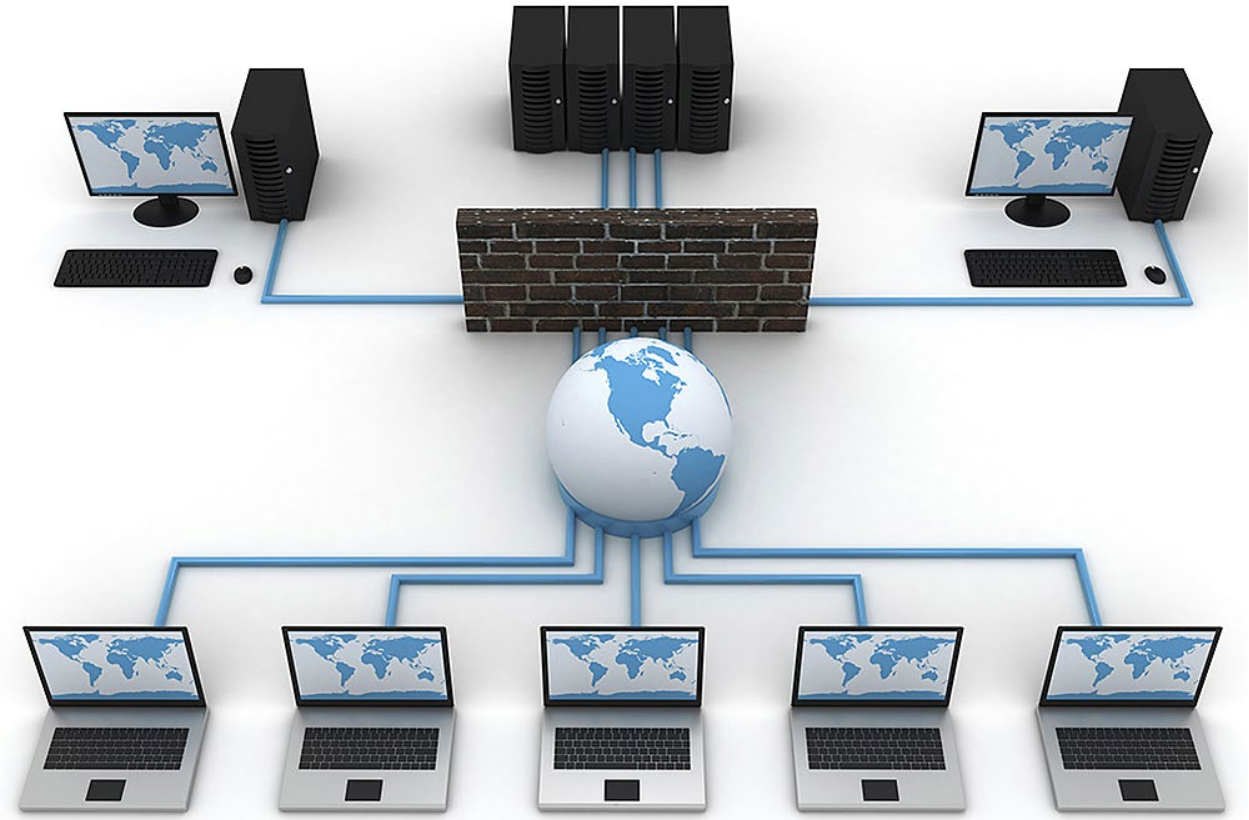
Work From Home & Telecommuting Policy

2024

Table of Contents

Work From Home (WFH) & Telecommuting Policy 2

Overview 2
Telecommuting resource misuse can have serious implications for an enterprise 3
Policy 4
Compensation and Benefits 5
Hours of Work 5
Attendance at Meetings 6
Sick Leave and Time Off 6
Workers' Compensation and Safety Program Liability 6
Equipment and Supplies 6
Record Management Process and BCP 7
BYOD Security 7
Telecommuting costs 8
Work From Home 10
Appendix 13
Employer Legal Workplace Responsibilities 14
Position Requirements for Qualification for WFH & Telecommuting 15
Top 10 Best Practices 16
Job Description 17
Manager Telecommuting
Manager Work From Home Support
Electronic Forms 18
Company Asset Control Log
Inspection Checklist Alternative Loction
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 19



Job Descriptions

Table of Contents

The following pages contain the full job descriptions for these 17 positions.

- Chief Compliance Officer
- Chief Experience Officer
- 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

Chief Compliance Officer (CCO)

Position Purpose

The Corporate Compliance Officer's role is to oversee and review all legal technology issues across the organization. This includes providing objective assessments of the company's compliance with legislation governing the organization's information technology systems and industry-specific regulations. The Corporate Compliance Officer also directs the development and implementation of policies and procedures to ensure that the organization's practices remain observant of all pertinent local, state/province/county, and federal laws.

The Chief Compliance Officer oversees the Corporate Compliance Program, functioning as an independent and objective body that reviews and evaluates compliance issues/concerns within the organization. The position ensures the Board of Directors, management and employees comply with the rules and regulations of regulatory agencies, that company policies and procedures are being followed, and that behavior in the organization meets the company's Standards of Conduct.

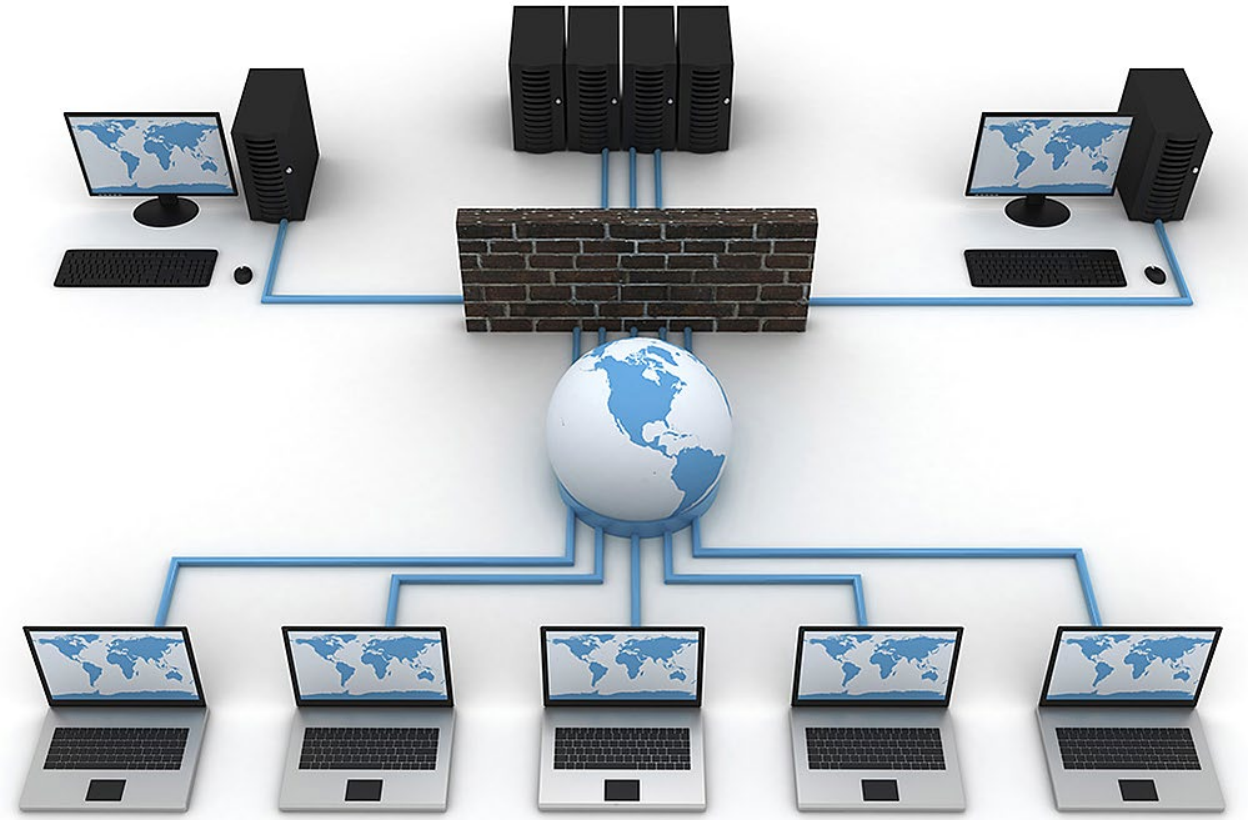
The Corporate Compliance Office exists:

- As a channel of communication to receive and direct compliance issues to appropriate resources for investigation and resolution, and
- As a final internal resource with which concerned parties may communicate through other formal channels and resources have been exhausted.

The Chief Compliance Officer (CCO) is responsible for the overall direction of all compliance issues associated with Information Technology applications, communications (voice and data), and computing services within the enterprise. At the same time, the CCO 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.

The CCO 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.

The CCO oversees and coordinates compliance efforts across the enterprise, including information technology, human resources, communications, legal, facilities management, and other groups, to identify security initiatives and standards. The CCO works closely with the chief information officer and the chief security officer and must have a strong working knowledge of information technology.



Forms

Table of Contents

The following pages contain the forms to support these policies and procedures

- Disaster Recovery
    - Location Contact Numbers
- Record Management
    - Administrative Records
    - Computer and Information Security Records
    - Computer Operations and Technical Support
    - Data Administration
    - Facility Records
    - Financial Records
    - General Systems and Application Development
    - Mobile Device Access and Use Agreement
    - Network and Communication Services
    - Personnel Records
    - Safety Records
    - Sales Records
    - User and Office Automation Support
- Security
    - Mobile Device Access and Use Agreement
    - Mobile Device Security and Compliance Checklist
    - Privacy Compliance Policy Acceptance Agreement
    - Security Access Application
    - Sensitive Information Policy Compliance Agreement
    - Server Registration
    - Telecommuting Work Agreement
    - Text Messaging Sensitive Information Agreement
    - Work From Home Work Agreement
- Others
    - BYOD Access and Use Agreement
    - Company Asset Employee Control Log
    - Internet and Electronic Communication
    - Social Networking Policy Compliance
    - Telecommuting IT Checklist
    - Telecommuting Work Agreement
    - Wearable Device Access and Use Agreement
    - Work From Home Contact Information
    - Work From Home IT Checklist

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 – The 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 files 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.