Security Manual Template

Janco Associates, Inc.

2025

Table of Contents

Appendix - A

Security - Introduction

This document defines a formal, ENTERPRISE-wide program intended to protect Information and data, including Internet and Information Technology systems, resources and assure their availability to support all ENTERPRISE operations.

All elements of the ENTERPRISE Security Program should be structured to minimize or prevent damage, which might result from accidental or intentional events, or actions that might breach the confidentiality of ENTERPRISE records, result in fraud or abuse, or delay the accomplishment of ENTERPRISE operations.

The objective of the ENTERPRISE Security Program is to achieve an effective and cost-beneficial security posture for the enterprise's Internet and Information Technology systems. Attainment of this objective requires a balanced combination of problem recognition, resources, and policy to implement an effective program.

The information in this manual:

- Applies to all systems[1] and must be considered from a total-system perspective (i.e., the protection of information must be considered from its origination to its final destruction, to include all processes affecting the information)
- Should be considered as the minimum standard for all systems and supporting manual activities
- Establishes security policies, assigns responsibilities, and prescribes procedures for the development and maintenance of ENTERPRISE-wide security
- Describes the ENTERPRISE security program
- Complies with the intent of prevailing privacy legislation regarding safeguards and with certain sections of the foreign corrupt practices act

[1] *This includes manual, Internet and Information technology systems.*

Scope

The scope of this manual is:

- Provides uniform policy and centralized guidance for dealing with all known and recognized aspects of security affecting ENTERPRISE and its operations
- Provides realistic guidance to ensure that all sensitive information handled by ENTERPRISE automated and manual systems is protected commensurate with the risk of inadvertent or deliberate disclosure, fraud, misappropriation, misuse, sabotage, or espionage
- Prevents damage to ENTERPRISE business operations due to unauthorized disclosures
- Assures the individual privacy of ENTERPRISE customers and staff members
- Protects funds, supplies, and materials from theft, fraud, misappropriation, or misuse
- Protects the property and rights of contractors, vendors, and other organizations
- Provides for the documented, justified selection of physical, technical, and administrative security controls that are cost-effective, prudent, and operationally efficient
- Provides for the monitoring of the implementation of selected security controls and procedures
- Provides for the auditing and reviewing functions necessary to ensure compliance with stated security requirements
- Protects contract negotiations and other privileged considerations in dealings with contractors, vendors, media reporters, and others
- Protects staff members from the unnecessary temptation to misuse ENTERPRISE resources while fulfilling their normal duties
- Protects staff members from suspicion in the event of misuse or abuse by others

tion assets

incidents of hardware,
ess, intentional abuse, or

siness interruptions and to

- Protects management from charges of imprudence in the event of a compromise of any security system or disaster

Objective

The objective of the ENTERPRISE Security Program is to create an ENTERPRISE environment where, based upon an active and continuous risk analysis program, the following elements of Internet and Information Technology Security can be successfully integrated and implemented:

- Denial of access to the Internet and Information Technology systems resources based upon a defined access requirement
- A proven ability to audit all transactions and processes impacting ENTERPRISE databases and operational outputs
- Both security awareness and staff member programs are designed to educate staff members about ENTERPRISE's security requirements.
- Traditional physical security controls and accountability with manual as well as automated processes
- Systems development review procedures and testing to ensure security in all Internet and Information Technology systems designs and procurements
- A program of management reviews and audits to ensure compliance with security controls
- A realistic and exercised contingency plan

Applicability

This manual and the ENTERPRISE Security Program apply to all ENTERPRISE activities, departments, and divisions processing and/or utilizing Internet and Information Technology systems r

The provi systems resources regardles

Internet a equipment, remote terminals services, staff members, suppliers, and facilities.

ISO Security Domains

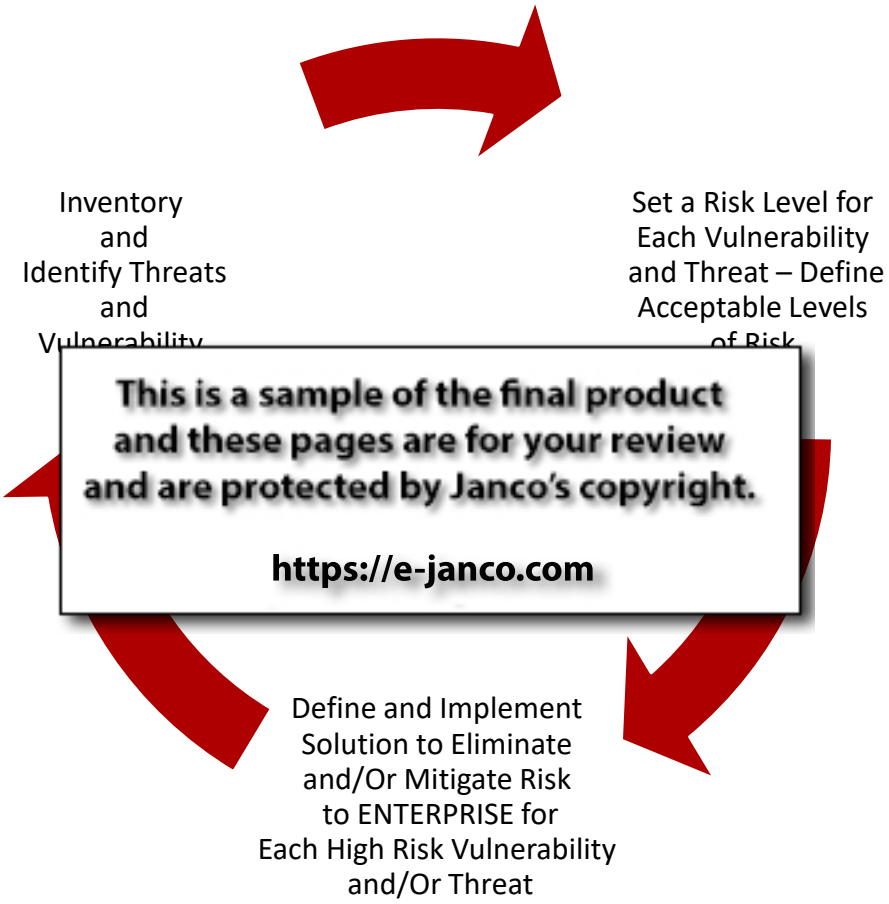
The ISO Domain standard is comprised of 11 distinct domains of information security. The Security Manual Template addresses each throughout the template with particular emphasis in the sections outlined below:

ISO Security Domain	Security Manual Template Sections
Security Policy	Security General Policy Chapter
Organization of Information Security	Responsibility Chapter
Asset Management	Insurance Chapter
Human Resources Security	Physical Control Chapter Facility design, construction, and operational considerations Chapter
Physical and Environmental Security	Physical Control Chapter Data and Software Security Chapter
Communications and Operations Management	Responsibilities Chapter
Access Control	Physical Control Chapter Access Control Chapter
Information Systems Acquisition, Development, and Maintenance	Processes, Forms, and Checklist - Appendix
Information Security Incident Management	Incident Reporting Procedure - Appendix
Business Continuity Management	Internet and IT Contingency Planning Chapter
Compliance	Minimum and Mandated Security Standards and Best Practices to Manage Compliance Chapters

The Ir ations on the
gover riginated from British
Stand 00 organizations
aroun mentation framework,
for int d certification
stand ols covering eleven
doma Management System
(ISMS). Further, ISO 27001 also specifies the Plan-Do-Check-Act (PDCA) model for continuous quality improvement, which is the same PDCA model used in ISO 9001 Total Quality Management (TQM) initiatives.

Vulnerability Analysis and Threat Assessment

The overall vulnerability analysis and threat assessment process is followed via a structured approach. It is the basis for identifying vulnerabilities and assessing the impacts of existing and new exposures that place ENTERPRISE at risk. The result of this process is to eliminate and/or mitigate unacceptable risk levels within the ENTERPRISE.



Threat / Vulnerability / Risk Process

Evaluate Risk

Risks are at both physical and electronic locations. The result should be a matrix that is used to identify threat areas via vulnerability analysis and business impact analysis tools. The result will be a matrix like the one shown below.

Risk Ranking

Impact of Loss	Vulnerability (Probability of Threat)					
	Will Occur over 90%	Extreme 90%< >75%	High 75%< >25%	Moderate 25%< >10%	Low	Under 10%
Catastrophic						
Very High						
Noticeable to ENTERPRISE						
Minor						
None						

Once every risk has been identified and analyzed using the same method of reporting, then ENTERPRISE can understand the existing situation.

The impact of a loss is defined as:

Catastrophic - as a result ENTERPRISE could cease to exist and/or would be placed

its material
e to ENTERPRISE's
ENTERPRISE's ability

vely and efficiently,

Minor - ENTERPRISE would be affected in a minor way with little productivity and/or service level loss.

None - No impact.

Impact of Loss	Risk Point Value				
	Will Occur over 90%	Extreme 90%< >75%	High 75%< >25%	Moderate 25%< >10%	Low Under 10%
Catastrophic	8	7	6	5	4
Very High	7	6	5	4	3
Noticeable to ENTERPRISE	6	5	4	3	2
Minor	5	4	3	2	1
None	0	0	0	0	0

Interpretation of scores	
6 to 8	These risks are extreme. Countermeasure actions to mitigate these risks should be implemented immediately.
5	These risks are very high. Countermeasure actions to mitigate these risks should be implemented as soon as possible.
3 to 4	These risks are moderate. Countermeasure actions to mitigate these risks should be implemented in the near term.
	e actions to emented as urity overall.
	uld continue to

Rights

All Internet and Information Technology systems resources should be assigned to an owner; however, this does not imply full rights of ownership (i.e., the enterprise retains the rights to authorize the sale, distribution, or destruction of a resource).

- The owner is the end-user or person responsible for the assets controlled by a system. Only the identified owner may authorize a user or group of users to access protected resources. Owners of resources are responsible for specifying the:
- A degree of protection for that resource
- Authorized users of that resource
- Access the authority of each user following the policies stated in this manual

		Systems	Applications
Data	Production	Development Group	End Users
	Test	Software Engineering	Application Support Group
Software	Production	Development Group	Development Group
	Test	Software Engineering	Application Support Group
Internet Intranet	Operation	ISP [11] Provider	Internet Support Group
	Development	ISP Provider	Internet Development Group
Commands	System Operation	Development Group	
Transactions			
Address Spac			
Docume			

Rights Matrix Table

Only the owner of a resource will have the authority to approve a change to the access control restrictions previously specified for that resource. Owners of data are responsible for reviewing access to that data. Owners are also responsible for determining the following resource characteristics:

- Value, importance, and specific business purpose
- Level of classification in one of the classes

[11] *ISP – Internet Service Provider this can be an internal group within the enterprise or an outsourced provider.*

Email Gateway for Ransomware Attacks

Email cyberattacks are as old as email itself. Ransomware attackers continue developing new tactics as security capabilities continue to become more robust. While 'click-and-run' attacks like spam and mass phishing campaigns still exist, Ransomware cyberattackers do not spend too much time crafting them and they can be effectively blocked with traditional security controls.

Type of Attack	Method	Techniques Used	Payload Delivery
Spam	Mass e-Mail	N/A	Malicious Link - executable
Mass Phishing	Mass e-Mail	Phishing Kits	Malicious Link - executable
Impersonations	Gmail/Yahoo look alike domains	Social Engineering	Ask/Request - fake attachment
Financial Fraud	Gmail/Yahoo look alike domains	Impersonations and Social Engineering	Ask/Request - fake attachment from bank or agency like IRS
Vendor Fraud	e-Mail from compromised account	Impersonations and Social Engineering	Ask/Request - fake attachment from know vendor
Credential Phishing	e-Mail from compromised account	Redirects, Impersonnations for login pages	Fake attchments - 0 day links
Account Takeover	Credential phishing attack	Auto-forwareding rules, lateral movement	Fake attchments - 0 day links

Some indicators of a ransomware attack are:

- a user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious;
- it (CPU) of a computer and disk
  nware searching for, encrypting, and
- re encrypts, deletes re-names, and/or
- between the ransomware and the
- command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

Measures that need to be included are:

- A security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronically protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- Procedures to guard against and detect malicious software;
- Train users on malicious software protection so they can assist in detecting malicious software and know-how to report such detections; and
- Access controls to limit access to ePHI to only those persons or software programs requiring access.

Appendix - A

Attached Job Descriptions

Chief Artificial Intelligence Officer (CAIO)
Chief Security Officer (CSO)
Chief Compliance Officer (CCO)
Data Protection Officer
Manager Security and Workstation
Manager WFH support
Security Architect
System Administrator

There is a more complete set in the Security Job Descriptions Bundle.
https://e-janco.com/jobdescriptions.html

Attached Policies

To ensure that you have the latest version of several critical IT Infrastructure policies (when this template updates), they are included as separate documents. However, be aware that you will NOT BE notified when the policies below are updated unless this Template is updated.

These policies are in a sub-directory title "Policy"

Blog and Personal Website Policy
Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy
Mobile Device Policy
Physical and Virtual File Server Security Policy
Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data
Travel and Off-Site Meeting Policy

There is a more comprehensive set in the IT Infrastructure Policy Bundle
https://e-janco.com/individual-policies.htm

Attached Security Forms

To ensure that you have the latest ve
this template updates), they are inclu
will NOT BE notified when the policie

These policies are in a sub-directory titled "Forms"

Application & File Server Inventory
Blog Policy Compliance Agreement
BYOD Access and Use Agreement
Company Asset Employee Control Log
Email Employee Agreement
Employee Termination Procedures and Checklist
FIPS 199 Assessment
Internet Access Request Form
Internet and Electronic Communication Employee Agreement
Internet use Approval
Mobile Device Access and Use Agreement
Mobile Device Security and Compliance Checklist
New Employee Security Acknowledgment and Release
Outsourcing and Cloud Security Compliance Agreement
Outsourcing Security Compliance Agreement
Preliminary Security Audit Checklist
Privacy Compliance Policy Acceptance Agreement
Risk Assessment
Security Access Application
Security Audit Report
Security Violation Procedures
Sensitive Information Policy Compliance Agreement
Server Registration
Social Networking Policy Compliance Agreement
Telecommuting Work Agreement
Text Messaging Sensitive Information Agreement
Threat and Vulnerability Assessment Inventory
Work From Home Work Agreement

Additional Attached Materials

Business and IT Impact Questionnaire

Attached as a separate document

Threat and Vulnerability Assessment Tool

Attached as a separate document

Sarbanes-Oxley Section 404 Check List Excel Spreadsheet

Attached as a separate document

Employee Termination Process

After an employee has been terminated (voluntary or involuntary) you can find yourself in the middle of a wrongful termination lawsuit. This can cost the company both time and money. If you are unlucky, you may be forced to hire the employee back. Using an employee termination checklist can help ensure you follow all the correct procedures when letting someone go.

As you now know, firing or laying off an employee is not as simple as saying "You're fired" or "You are laid off." There are legal ramifications and is therefore much more complicated than it appears on the surface.

- ❑ **Compile The Proper Documentation** You or your manager should have the right legal documents in place before you begin termination procedures. Be aware that the court of law. In other mpany policy.

urces Department. They r attorney reviews it.

e going to offer this Human Resources ould be. You should have meeting. Include a document for the employee to sign before they get the package, which limits or eliminates their rights to sue the company, its employees, and its agents.

- ❑ **Come Up With Additional Agreements** As an employer you may wish to have the employee sign an employee termination agreement or a non-compete agreement. Make sure that your draft is run by either your Human Resources Personnel or your business attorney.
- ❑ **Prepare An Agenda For The Termination Meeting** You must know exactly what you are going to say and how you will say it. Make sure you set up a meeting room ahead of time that is away from the individual's coworkers. Also, have another representative (witness) from the company there. Usually, a member of the Human Resources Department is a good choice.
- ❑ **List Out Those Items The Former Worker Must Return** Employee terminations are stressful for both the employer and the employee. During this time, you may forget to ask the worker to return important company property. Recovering it after the employee is gone will prove difficult.
- ❑ **Conduct An Employee Exit Interview** It is usually best to have a third party do this for you.

Firewall Security Policy Checklist

Identify which resources must be secure

- ❑ Mission Critical data and applications
- ❑ Backup data and applications
- ❑ Secondary data and applications
- ❑ Others

WAN security connections

- ❑ Wi-Fi
- ❑ BYOD
- ❑ Remote dial-in
- ❑ Site-to-Site VPN
- ❑ Employee connectivity
- ❑ Vendor connectivity
- ❑ Customer (Client) connectivity
- ❑ Business-to-business access

Network Documentation

Information Disclosure Policy

- ❑ What information is shared with others: Internally, externally, and public
- ❑ Mission-critical information and secondary information
- ❑ Who sets the guidelines for the information that is disclosed and the associated timing of its release

Disaster Recovery Business Continuity

- ❑ Documentation
- ❑ Priorities for restoration
- ❑ Security during event recovery
- ❑ Compliance requirements

Revision History

2025

- Updated to reflect the impact of AI
- Updated to meet the latest security requirements
- Include the latest Supply Chin Security Audit Program
- Updated all included electronic forms
- Updated all included Job Descriptions
- Updated all included Policies and tools

2024

- Added how to apply AI to Security Management
- Added job description for Chief AI Officer
- Added Mobile Device Security Options
- Updated to meet the latest security requirements
- Updated all included electronic forms
- Updated all included Job Descriptions

2023

- Updated to meet the latest security requirements
- Updated all included electronic forms
- Updated all included Job Descriptions

2022

- Updated to meet the IoT compliance mandates for IEC 62443
- Updated to meet the latest security requirements
- Updated all included electronic forms
- Updated all included Job Descriptions

2021 - Ransomware Update

- Updated the Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy to highlight Ransomware gateway email threats
    - System Administrator
- Updated job descriptions