Security Manual Template

Janco Associates, Inc.

Version 2023

Table of Contents

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.

total-system perspective (i.e., the origination to its final rmation)

systems and supporting manual

- 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
- ppropriation, or misuse
- ther organizations
- chnical, and
  t, and operationally

- 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
- Ensures the integrity and accuracy of all ENTERPRISE information assets
- Protect ENTERPRISE information processing operations from incidents of hardware, software, or network failure resulting from human carelessness, intentional abuse, or accidental misuse of the system
- Ensures the ability of all ENTERPRISE operations to survive business interruptions and to function adequately after recovery
- 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

esigned to educate staff

y with manual as well as

o ensure security in all Internet
urements

- 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 resources.

The provisions of this manual apply to all Internet and Information Technology systems resources regardless of application, functional organization, or source of funding.

Internet and Information Technology systems resources include all computer equipment, remote terminals, peripherals, data, software, associated documentation, contractual services, staff members, suppliers, and facilities.

ISO Security Domains

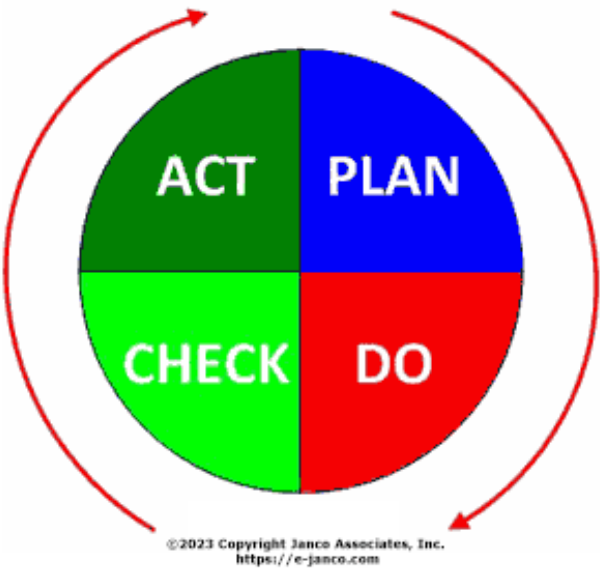
The International Standards Organization (ISO) has developed two specifications on the governance of information security, ISO 17799 and ISO 27001. Both have originated from British Standards, BS7799 parts 1 and 2, which have been used to certify over 2,500 organizations around the world. ISO 17799 is an international code of practice, or implementation framework, for information security best practices. ISO 27001 serves as the auditing and certification standard for the ISO 17799 framework with 133 information security controls covering eleven domains and specifies how to design an ISO-certified Information Security 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. According to the Institute of Internal Auditors (IIA), the PDCA cycle helps "the organization to know how far and how well it has progressed" and "influences the time and cost estimates to achieve compliance." BSI Management Systems, the world's largest ISO certification body and the author of BS7799 standards, defined the ISMS as "a systematic approach to managing sensitive company information so that it remains secure. ISMS encompasses people, processes, and IT systems."

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**
• Orga	• **pter**
• Asse	
• Hum	• **hapter** • **nstruction, and** • **derations Chapter**
• Phys	• **hapter** • **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**

development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

ISO 27003 – This is a PROPOSED Standard, which has yet to be completely defined. This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (Information Security Management System). The purpose of this proposed development is to provide help and guidance in implementing ISMS. This will be a quality control standard when it is released. ISO 27003 will focus on utilizing the Plan-Do-Act-Check (PDCA) method when establishing, implementing, reviewing, and improving the ISMS.



ISO 27004 - This is the designated number for a PROPOSED standard covering information security, system management, measurement, and metrics.

ndard covering information
SO 27000 series, no firm
the ISMS risk management
ilities. This is the ISO number
agement.

rganizations that offer

Information is an asset that, like other important business assets, is essential to an enterprises' business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. Because of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see OECD Guidelines for the Security of Information Systems and Networks).

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.

Impact of a loss is defined as:

r would be placed

s material
to ENTERPRISE's
NTERPRISE's ability

ly 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.
	tions to nted as overall.
	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	**Operation**	ISP [11] Provider	Internet Support Group
Intranet	**Development**	ISP Provider	Internet Development Group
Commands	**System Operation**	Development Group	
	System Maintenance	Software Engineering	
			oup
			oup

On ge 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:

attachment opened, or a

PU) of a computer and disk
e searching for, encrypting, and

ncrypts, deletes and re-names, and/or relocates data; and

- detection of suspicious network communications between the ransomware and the attackers'
- 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 Security Officer (CSO)

Chief Compliance Officer (CCO)

Data Protection Officer

Manager Security and Workstation

Manager WFH support

Security Architect

System Administrator

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

Attached Security Forms

To ensure that you have the latest version of several critical Security Management Forms (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 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

Revision History

2023 Edition

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

Version 2022

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

Version 2021 - Ransomware Update

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

Version 2021

- Updated to meet the latest compliance mandates including CCPA and GDPR
- Updated to meet WFH security requirements
- Updated all 28 included electronic forms
- Added form
  - Work From Home Work Agreement
- Added job descriptions
  - Data Protection Officer
  - Manager Security and Workstation
  - Manager WFH support
  - Security Architect
  - System Administrator
- Updated job descriptions

Version 2020

- Updated to meet the latest compliance mandates including CCPA
- Included job descriptions
  - Chief Security Officer (CSO)
  - Chief Compliance Officer (CCO)
- Included Policy – Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy as a standalone item.
- Updated all electronic forms to current versions
- Updated all attached policies to current versions

Version 2019

- Updated to meet the latest compliance mandates
- Updated forms as a separate attached PDF file
- Updated all attached policies as separate items

Version 2018 - 07

- Added section to cover the New California Consumer Privacy Act – Defines consumer rights and business responsibilities.
- Change the Version numbering system for the Security Manual Template