

Security Manual Template

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>



2024

Table of Contents

Security - Introduction	6
Scope	7
Objective	8
Applicability.....	8
Best Practices.....	9
WFH Operational Rules.....	16
Web Site Security Flaws	17
ISO 27000 Compliance Process	19
Security General Policy	21
Responsibilities.....	24
Minimum and Mandated Security Standard Requirements	28
ISO Security Domains	30
ISO 27000.....	31
IEC 62443.....	38
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999.....	39
FTC Information Safeguards	39
Federal Information Processing Standard – FIPS 199	40
NIST SP 800-53	44
Sarbanes-Oxley Act.....	45
California SB 1386 Personal Information Privacy	45
California Consumer Privacy Act	45
Massachusetts 201 CMR 17.00 Data Protection Requirements.....	46
What Google and Other 3 rd Parties Know	47
Internet Security Myths	48
Vulnerability Analysis and Threat Assessment	50
Threat and Vulnerability Assessment Tool	51
Evaluate Risk.....	55
Risk Analysis – IT Applications and Functions	57
Objective	57
Roles and Responsibilities.....	58
Program Requirements.....	59
Frequency.....	60
Relationship to Effective Security Design.....	60
Selection of Safeguards.....	60
Requests for Waiver.....	61
Program Basic Elements	61
Staff Member Roles	66
Basic Policies	67
Security - Responsibilities	68
Determining Sensitive Internet and Information Technology Systems Positions	69
Personnel Practices.....	70
Education and Training.....	74
Contractor Personnel.....	75

Physical Security	76
Information Processing Area Classification.....	76
Classification Categories	77
Access Control	78
Levels of Access Authority	79
Access Control Requirements by Category	81
Implementation Requirements	81
Protection of Supporting Utilities	82
Facility Design, Construction, and Operational Considerations.....	83
Building Location	83
External Characteristics	84
Location of Information Processing Areas.....	85
Construction Standards	85
Water Damage Protection.....	86
Air Conditioning	86
Entrances and Exits.....	87
Interior Furnishings.....	87
Fire	88
Electrical	92
Air Conditioning	93
Remote Internet and Information Technology Workstations.....	93
Lost Equipment	94
Training, Drills, Maintenance, and Testing	95
Media and Documentation	96
Data Storage and Media Protection.....	96
Documentation	97
Data and Software Security	99
How to Apply Artificial Intelligence to Security Management	99
Resources to Be Protected	100
Classification	102
Rights.....	104
Access Control.....	105
Internet / Intranet / Terminal Access / Wireless Access.....	109
Spyware.....	112
Wi-Fi Security Standards.....	114
Logging and Audit Trail Requirements.....	116
Satisfactory Compliance.....	120
Violation Reporting and Follow-Up.....	120
Internet and Information Technology Contingency Planning	121
Responsibilities	121
Information Technology	122
Contingency Planning.....	123
Documentation	124
Contingency Plan Activation and Recovery	125
Disaster Recovery / Business Continuity and Security Basics	126

Insurance Requirements.....	130
Objectives.....	130
Responsibilities.....	130
Filing a Proof of Loss.....	131
Risk Analysis Program.....	131
Purchased Equipment and Systems.....	132
Leased Equipment and Systems.....	132
Media.....	133
Business Interruption.....	133
Staff Member Dishonesty.....	134
Errors and Omissions.....	134
Security Information and Event Management (SIEM).....	135
Best Practices for SIEM.....	136
KPI Metrics for SIEM.....	137
Identity Protection.....	138
Identifying Relevant Red Flags.....	138
Preventing and Mitigating Identity Theft.....	138
Updating the Program.....	139
Methods for Administering the Program.....	139
Ransomware – HIPAA Guidance.....	140
Email Gateway for Ransomware Attacks.....	141
Required Response.....	142
Outsourced Services.....	143
Responsibilities.....	144
Outside Service Providers – Including Cloud.....	145
Waiver Procedures.....	147
Purpose and Scope.....	147
Policy.....	147
Definition.....	147
Responsibilities.....	147
Procedure.....	148
Incident Reporting Procedure.....	149
Purpose & Scope.....	149
Definitions.....	149
Responsibilities.....	149
Procedure.....	150
Analysis/Evaluation.....	151
Access Control Guidelines.....	152
Purpose & Scope.....	152
Objectives.....	152
Definitions of Access Control Zones.....	153
Responsibilities.....	154
Badge Issuance.....	157

Appendix - A	159
Attached Job Descriptions.....	159
Chief Artificial Intelligence Officer (CAIO)	159
Chief Security Officer (CSO).....	159
Chief Compliance Officer (CCO)	159
Data Protection Officer	159
Manager Security and Workstation.....	159
Manager WFH support	159
Security Architect.....	159
System Administrator	159
Attached Policies.....	159
Blog and Personal Website Policy	159
Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy	159
Mobile Device Policy.....	159
Physical and Virtual File Server Security Policy	159
Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data	159
Travel and Off-Site Meeting Policy.....	159
Attached Security Forms.....	160
Application & File Server Inventory	160
Blog Policy Compliance Agreement.....	160
BYOD Access and Use Agreement	160
Company Asset Employee Control Log.....	160
Email Employee Agreement	160
Employee Termination Procedures and Checklist.....	160
FIPS 199 Assessment	160
Internet Access Request Form	160
Internet and Electronic Communication Employee Agreement.....	160
Internet use Approval	160
Mobile Device Access and Use Agreement	160
Mobile Device Security and Compliance Checklist	160
New Employee Security Acknowledgment and Release	160
Outsourcing and Cloud Security Compliance Agreement	160
Outsourcing Security Compliance Agreement	160
Preliminary Security Audit Checklist.....	160
Privacy Compliance Policy Acceptance Agreement.....	160
Risk Assessment	160
Security Access Application.....	160
Security Audit Report	160
Security Violation Procedures.....	160
Sensitive Information Policy Compliance Agreement.....	160
Server Registration	160
Social networking Policy Compliance Agreement	160
Telecommuting Work Agreement	160
Text Messaging Sensitive Information Agreement	160
Threat and Vulnerability Assessment Inventory.....	160
Work From Home Work Agreement.....	160

Additional Attached Materials	161
Business and IT Impact Questionnaire	161
Threat and Vulnerability Assessment Tool.....	161
Sarbanes-Oxley Section 404 Check List Excel Spreadsheet.....	161
Appendix - B	162
Practical Tips for Prevention of Security Breaches and PCI Audit Failure.....	162
Risk Assessment Process	167
Employee Termination Process.....	170
Security Management Compliance Checklist	174
Massachusetts 201 CMR 17 Compliance Checklist	177
User/Customer Sensitive Information and Privacy Bill of Rights	179
General Data Protection Regulation (GDPR) - Checklist.....	180
Firewall Security Requirements	205
Firewall Security Policy Checklist	207
BYOD and Mobile Content Best of Breed Security Checklist.....	208
Revision History	210

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

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 systems¹ 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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

- ✦ 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
- ✚ Both security awareness and staff member programs designed to educate staff members in ENTERPRISE's security requirements
- ✚ Traditional physical security controls and accountability with manual as well as automated processes

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

to ensure security in all Internet
requirements
re compliance with security

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 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

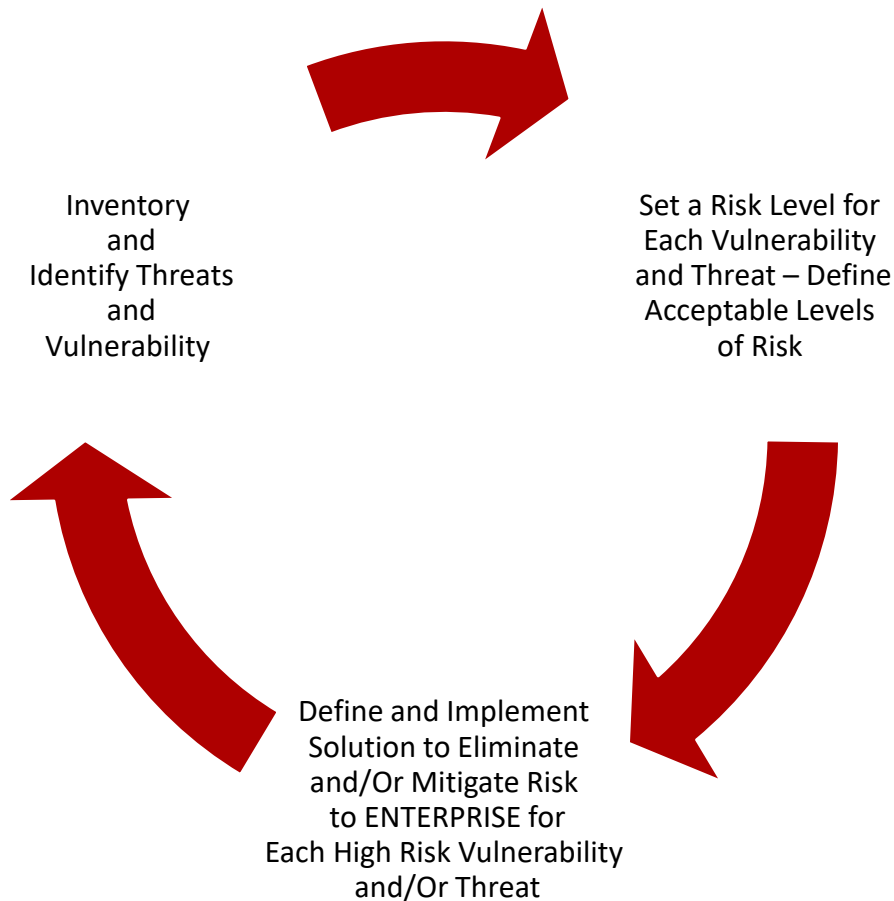
This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

specifications on the have originated from British er 2,500 organizations mplementation framework, ing and certification controls covering eleven 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.

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

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

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)				Low	Under 10%
	Will Occur over 90%	Extreme 90% < >75%	High 75% < >25%	Moderate 25% < >10%		
<i>Catastrophic</i>						
<i>Very High</i>						
<i>Noticeable to ENTERPRISE</i>						
<i>Minor</i>						
<i>None</i>						

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:

Catastrophic - as a result ENTERPRISE could cease to exist and/or would be placed in a position where it would be unable to continue its operations.

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

Very High - as a result ENTERPRISE's ability to continue its operations would be severely affected.

Noticeable to ENTERPRISE - as a result ENTERPRISE's ability to continue its operations would be noticeably affected.

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

None - No impact.

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%
<i>Catastrophic</i>	8	7	6	5	4
<i>Very High</i>	7	6	5	4	3
<i>Noticeable to ENTERPRISE</i>	6	5	4	3	2
<i>Minor</i>	5	4	3	2	1
<i>None</i>	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.
1 to 2	These risks are low. Countermeasure actions to mitigate these risks should be implemented as convenient as they will enhance security overall.
0	These currently pose no risk but should continue to be monitored.

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

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	
Transactions	Production	Development Group	
	Test	Application Support Group	
Address Space (Capacity)		Development Group	
Documentation		Application Support Group	

Rights Matrix Table

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

rove a change to the access control of data are responsible for reviewing hining the following resource

ose

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

Email Gateway for Ransomware Attacks

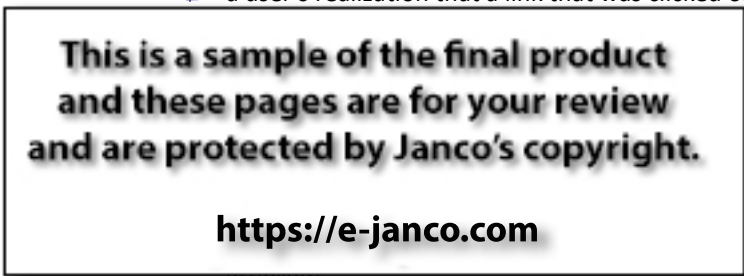
Email cyberattacks are as old as email itself. Ransomware attackers continue developing new tactics as security capabilities continue to become more robust. While ‘click-and-run’ attacks like spam and mass phishing campaigns still exist, Ransomware cyberattackers do not spend too much time crafting them 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, Impersonations for login pages	Fake attachments - 0 day links
Account Takeover	Credential phishing attack	Auto-forwarding rules, lateral movement	Fake attachments - 0 day links

© 2023 Copyright Janco Associates, Inc. - <https://e-janco.com>

Some indicators of a ransomware attack are:

- ✚ a user’s realization that a link that was clicked on, a file attachment opened, or a



- ✚ 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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

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*

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

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

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

Revision History

2024

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

2023

- ✚ Updated to meet 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 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

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