

**Sarbanes-Oxley
PCI-DSS CobiT
ISO 27000 -HIPAA - ITIL
FIPS 199 - NIST SP 800-53**

Security Manual Template

Version 10.0

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Table of Contents

Security - Introduction	7
Scope	8
Objective.....	9
Applicability	9
Best Practices When Implementing Security Policies and Procedures.....	10
Web Site Security Flaws	10
ISO 27000 Compliance Process	12
Security General Policy	13
Responsibilities	17

Minimum and Mandated Security Standard Requirements.....	20
Best Practices to Meet Compliance Requirements	34
Best Practices to Manage Compliance Violations	35
Best Data Destruction and Retention Practices	35
What Google Knows	36
Internet Security Myths	36

Vulnerability Analysis and Threat Assessment	39
Threat and Vulnerability Assessment Tool.....	40
Evaluate Risk	43

Risk Analysis – IT Applications and Functions.....	45
Objective.....	45
Roles and Responsibilities.....	46
Program Requirements.....	47
Frequency	47
Relationship to Effective Security Design.....	47
Selection of Safeguards.....	48
Requests for Waiver	48
Program Basic Elements	48

Staff Member Roles	53
Basic Policies	54
Security - Responsibilities	55
Determining Sensitive Internet and Information Technology Systems Positions.....	56
Personnel Practices.....	57
Education and Training	60
Contractor Personnel.....	60

Physical Security	61
Information Processing Area Classification.....	61
Classification Categories	62
Access Control	63
Levels of Access Authority	64
Access Control Requirements by Category	65
Implementation Requirements.....	65
Protection of Supporting Utilities	67

Facility Design, Construction and Operational Considerations	68
Building Location	68
External Characteristics	69
Location of Information Processing Areas	69
Construction Standards	70
Water Damage Protection	70
Air Conditioning	71
Entrances and Exits	71
Interior Furnishings.....	72
Fire.....	72
Electrical	76
Air Conditioning	77
Remote Internet and Information Technology Workstations	77
Lost Equipment.....	78
Training, Drills, Maintenance and Testing.....	78
<hr/>	
Media and Documentation	80
Data Storage and Media Protection.....	80
Documentation.....	81
<hr/>	
Data and Software Security	83
Resources to Be Protected.....	83
Classification	85
Rights	86
Access Control	87
Internet / Intranet / Terminal Access / Wireless Access	91
Spyware	93
Wireless Security Standards.....	95
Logging and Audit Trail Requirements	97
Satisfactory Compliance	101
Violation Reporting and Follow-Up.....	101
<hr/>	
Network Security	103
Vulnerabilities	103
Exploitation Techniques.....	103
Goal	104
Responsibilities	104
Resource Protection	105
Configuration Management.....	107
Dial-Up Controls.....	107
Message Authentication	107
Encryption.....	108
Network Contingency Planning.....	110
<hr/>	
Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data	111
Policy	111
Secure Network Standards	114
Email Retention Compliance.....	128
Privacy Guidelines.....	132
Best Practices.....	132

Internet and Information Technology Contingency Planning	134
Responsibilities	134
Information Technology	135
Contingency Planning	136
Documentation	137
Contingency Plan Activation and Recovery	137
Disaster Recovery / Business Continuity and Security Basics	138

Insurance Requirements	142
Objectives	142
Responsibilities	142
Filing a Proof of Loss	143
Risk Analysis Program	143
Purchased Equipment and Systems	143
Leased Equipment and Systems	144
Media	144
Business Interruption	145
Staff Member Dishonesty	145
Errors and Omissions	146

Outsourced Services	147
Responsibilities	147
Outside Service Providers	149

Travel and Off-Site Meetings	150
Laptop and PDA Security	150
Wireless & VPN	150
Maximize Data and Application Security	151
Minimize Attention	151
Carefully Use Shared Resources	152
Off-Site Meeting Special Considerations	152

Waiver Procedures	153
Purpose and Scope	153
Policy	153
Definition	153
Responsibilities	153
Procedure	154

Incident Reporting Procedure	155
Purpose & Scope	155
Definitions	155
Responsibilities	155
Procedure	156
Analysis/Evaluation	157

Access Control Guidelines	158
Purpose & Scope	158
Objectives	158
Definitions of Access Control Zones	159
Responsibilities	159
Badge Issuance	163

Internet, Email, and Electronic Communication	165
Overview	165
Internet and Electronic Communication Policy	170
Email	173
<hr/>	
Blog and Personal Web Sites Policy	176
Policy	176
Rights to content	177
Personal Website and Blog Guidelines – Non ENTERPRISE domains	180
Security Standards	181
<hr/>	
Mobile Access and Use Policy	182
Overview	182
Policy	182
<hr/>	
Processes, Forms, and Checklists	187
Security Violation Reporting	188
Security Audit Report Form	194
Preliminary Audit Security Checklist	195
New Employee Security Acknowledgement and Release	198
Internet & Electronic Communication - Employee Acknowledgment.....	199
Email - Employee Acknowledgment.....	200
Internet Use Approval.....	201
Internet Access Request	203
Security Access Application Form	204
Blog Policy Compliance Agreement	205
Mobile Device Access and Use Agreement	206
Company Asset Employee Control Log	207
Employee Termination Process.....	208
<hr/>	
Supporting Materials	212
Security Management Compliance Checklist	213
Massachusetts 201 CMR 17 Compliance Checklist	216
HIPAA Audit Program Guide	218
ISO 27000 Security Process Audit Checklist	222
1. Business and IT Impact Questionnaire	238
2. Threat and Vulnerability Assessment Tool	238
3. Sarbanes-Oxley Section 404 Check List Excel Spreadsheet	238
<hr/>	
Revision History	240

Security - Introduction

This document implements 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
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

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 property and rights of contractors, vendors and other organizations
- ✦ Provides for the documented, justified selection of physical, technical and administrative security controls which 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, correspondents and other organizations
- ✦ Protects staff members from 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 compromise of any security system or disaster

**This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

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 Internet and Information Technology systems resources based upon a defined access requirement
- ✦ A proven ability to audit all transactions and processes impacting ENTERPRISE data bases and operational outputs
- ✦ Both security awareness and staff member programs designed to educate staff members in the 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 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, supplies and facilities.

**This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

Best Practices When Implementing Security Policies and Procedures

After determining the best security policies and procedures, the implementation and deployment of security technologies into the organization begins. This is not a trivial exercise and – if done without both upper management support and end user understanding – one that will fail.

Best practices around security policy and procedure deployment include:

Practice – It is imperative that any solution be tested before implementation. Every environment is different and some solutions may interfere with business critical processes. It is important to understand the unintended results of implementing a security process before making it required.

Upper Management Approval – Upper management must not only be aware of upcoming security initiatives, but most support them wholeheartedly. This is critical when human resource policies come into play that could affect personnel. Upper management support will be necessary to enforce process that may be time consuming or require additional resources.

**This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

...ing changes to security processes.
...n and legitimate frustration. Users
...; put in place to ensure that business

...human resource policies – Ultimately, human resource policies have to be applied to ensure compliance with security policies. Security processes are often seen as obstructive and employees may try to avoid or circumvent technological solutions. It is imperative that human resource policies are in place to discipline these actions.

Web Site Security Flaws

Janco has identified top security flaws in “enterprise” web sites. They are:

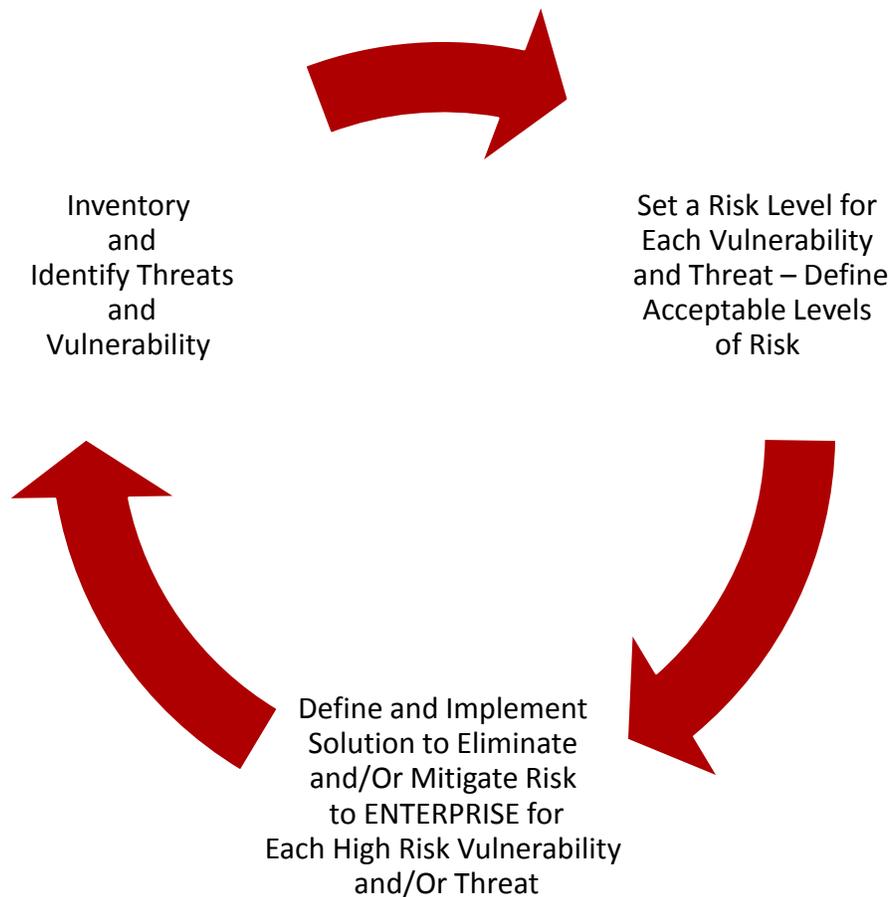
Using only single level verification for access to sensitive data - Password authentication is more easily cracked than cryptographic key-based authentication. The purpose of a password is to make it easier to remember the login credentials needed to access a secure resource, however biometric or key-based authentication is a stronger authentication method which make credential more difficult to crack.

Having “public” workstations or access point is connected to a secure network - If workstation that anyone can use or re-boot is connected to a secure resource you can't guarantee it is secure. Keyloggers, compromised network encryption clients, and other tricks of the malicious security cracker's trade can all allow someone unauthorized access to sensitive data regardless of all the secured networks, encrypted communications, and other networking protections you employ.

Sharing login credentials - The more login credentials are shared, the more they likely they are commonly know by too many others, even with people who should not have access to the system. The more they are shared, the more difficult it is to establish an audit trail to help track down the source of a problem. The more they are shared, the greater the number of people affected when logins need to be changed due to a security breach or threat.

Vulnerability Analysis and Threat Assessment

The overall vulnerability analysis and threat assessment process is one that 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 un-acceptable risk levels within ENTERPRISE.



Threat / Vulnerability / Risk Process

**This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

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%
<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 has the ability to 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 material legal and/or financial jeopardy.

Very High - as a result ENTERPRISE would not be able to meet its material contractual and/or service obligations. Or do material damage to ENTERPRISE’s reputation and have major negative long term implications on ENTERPRISE’s ability to continue being a going concern.

Noticeable - ENTERPRISE would not be able to operate effectively and efficiently, thus reducing productivity and service levels.

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

None - No impact.

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

PCI-DSS Compliance Table

* Th
PCI I
pers
prac
proc

**This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED**

Account Number). This protection must be consistent with
, other legislation (for example, related to consumer
rotection of this data or proper disclosure of a company's
ess. PCI DSS, however, does not apply if PANs are not stored,

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

The PCI DSS requirements 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 cardholder data environment

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

<i>Regulation</i>	<i>Industry Impacted</i>	<i>Retention Implications</i>	<i>Penalties</i>
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

Regulations and Industry Impact Table

Preliminary Audit Security Checklist

Page 1 of 3

Name	_____	Date	Click here to enter a date.
Phone	_____	Work Site	_____
Email	_____	Location	_____

General

<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Security Procedures are documented
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Employees are trained in Security Procedures
This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED	
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Fire Protection Equipment testing / certification is current
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Flammable liquids are safely stored

Comments:

Employees

<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Attentive
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	No employees work alone in this area on any shift?
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	Did not observe or hear of any security risks due to employee behavior?

Comments:

Employee Termination Checklist

Employee Name _____ ID Number _____
 Forwarding _____ Last Day [Click here to enter a date.](#)
 Address _____ Worked _____
 Phone Number _____
 Supervisor _____ Department _____

Instructions: Place your initials and next to the action taken

Termination Type

Voluntary Termination

_____ Written Resignation Letter

Other : _____

_____ Supporting Documentation

Involuntary Termination

_____ Corrective Action Followed

_____ Employee explanation provided

_____ HR Reviewed Information

_____ Letter of termination included reasons

<p>F This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED</p> <p>_____ How references will be handled</p> <p>_____ Subsequent access to premises</p> <p>_____ Rehire Eligibility <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Give to Employee (Optional)</p> <p>_____ Exit Interview</p> <p>_____ Benefits Book</p> <p>_____ Contact Information for HR</p> <p>_____ Contact Information for Department</p> <p>Other</p> <p>_____ Clean Work Area – Personal Belongings Removed</p> <p>_____ Process Electronic Termination From Systems</p> <p>Notes:</p>	<p>ect From Employee</p> <p>_____ Keys (building, desk, etc)</p> <p>_____ Badges – Security Cards</p> <p>_____ Cell Phones Pagers</p> <p>_____ Personal Computers</p> <p>_____ Credit Cards</p> <p>_____ Company Manuals / Documents</p> <p>_____ Parking Cards</p> <p>_____ Time Card</p> <p>_____ Expense Reports</p> <p>_____ Other: _____</p> <p>Cancel</p> <p>_____ Computer/Network Access</p> <p>_____ Long Distance Authorization</p> <p>_____ Email account</p> <p>_____ Phone List</p> <p>_____ Credit Cards</p> <p>_____ Security Codes</p> <p>_____ Direct Deposit</p>
--	--

Signature _____ Date _____

Revision History

Version 10.0 October 2012

- + Added section on FIPS 199
- + Added section on NIS SP 800-53
- + Added Electronic Forms
 - o FIPS 199 Assessment Electronic Form

Version 9.2 March 2012

- + Updated the Threat and Vulnerability Assessment to include mobile devices and BYODs
- + Added Electronic form
 - o BYOD Access and Use Agreement

Version 9.1 January 2012

- + Added Electronic form
 - o Employee Termination Checklist
- + Added Best Practices Section to Meet Compliance Requirements

Version 9.0 September 2011

- + Updated Sensitive Information Policy
- + Added Electronic Forms
 - o Blog Policy Compliance
 - o Company Asset Employee Control Log
 - o Email - Employee Acknowledgment
 - o Internet Access Request
 - o Internet Use Approval
 - o Internet & Electronic Communication - Employee Acknowledgment
 - o Mobile Device Access and Use Agreement
 - o New Employee Security Acknowledgement and Release
 - o Preliminary Security Audit Checklist
 - o Security Access Application
 - o Security Audit Report
 - o Security Violation Reporting
 - o Sensitive Information Policy Compliance Agreement

Version 8.3 May 2011

- ✚ Added policy for Mobile Device Access and Use
- ✚ Added Mobil Device Assess and Use Agreement Form
- ✚ Added Enterprise Owned Equipment Inventory Form
- ✚ Updated CSS Style sheet

Versaion 8.2 February 2011

- ✚ Updated the Threat and Vulneralbility Assessment Tool

Version 8.1 January 2011

- ✚ Add section on Best Practices When Implementing Security Policies and Procedures.
- ✚ Added section on Skype
- ✚ Updated Sensitive Information section
- ✚ Added section on enterprise web site security flaws
- ✚ Corrected minor errata

Version 8.0

- ✚ Updated Fire Suppression Section
- ✚ Updated for ISO compliance and security domain definition
Log management section expanded

Version 7.3

- ✚ Updated Business and IT Impact Questionnaire
 - Updated for COBIT compliance
 - Updated for PCI-DSS compliance
 - Updated for US state level compliance (New York, Massachusetts, and California)\
 - Update for ISO security requirements

Version 7.2

- ✚ Updated to comply with CobiT requirements
- ✚ Added Security Management Compliance Checklist
- ✚ Added Massachusetts Data Protection Requirements Section
- ✚ Added Massachusetts 201 CMR 17 Compliance Checklist

Version 7.1 - September 2009

- ✚ Corrected minor errata
- ✚ Added Employee Termination Process
- ✚ Added Employee Termination Checklist
- ✚ Forms Added
 - Employee Termination Form

Version 7.0

- ✚ Update to reflect latest PCI-DSS requirements
- ✚ Forms Updated
 - Security Violation Form
 - Inspection Checklist
 - New Employee Security Form
 - Internet & Electronic Communication - Employee Acknowledgment (short form)
 - Internet Use Approval Form
 - Internet Access Request Form
 - Security Access Application Form
- ✚ Updated ISO 27000 Security Process Audit Checklist
- ✚ Updated to CSS Style Sheet

Version 6.5

- ✚ Updated Threat and Vulnerability Assessment tool to include a detail work plan for the assessment process.
- ✚ Updated Threat and Vulnerability Assessment tool to include a definition of the safeguards that should be included.
- ✚ Threat and Vulnerability Assessment tool provided in PDF, WORD 2003, WORD 2007, EXCEL 2003, and EXCEL 2007 formats.

Version 6.4

- ✚ Blog Policy and Bog Forms added
- ✚ WORD 2007 Style Sheet Added

Version 6.3

- ✚ Best Practices Updated
- ✚ Added section with a summary of the ISO 27000 Series standards
- ✚ Updated the template to comply with ISO 27000 Series Standards (27001 and 27002)
- ✚ Disaster Recovery Plan Basics Section Added
- ✚ Wireless Security Standards Added
- ✚ Updated Business Impact and IT Questionnaire
- ✚ Corrected various errata

Version 6.2

- + Sensitive Information Policy Updated
- + Best Practices Added
- + Wireless and VPN Added
- + Payment Card Industry Data Security Standard Added
- + Added separate document PCI DSS Audit Program
- + Internet and Email Communication Updated
- + Email Forwarding Added
- + Travel, Laptop, PDA, and Off-Site Meetings Updated
- + Laptop and PDA Security Added
- + Wireless and VPN Added

Version 6.1

- + Added HIPAA Audit Program
- + Added ISO 17799 Security Audit Check List

Version 6.0

- + Added section defining ISO 17799 requirements
- + Modified entire template to be ISO 17799 compliant
- + Added Best Data Deletion and Retention Practices
- + Added Spyware Best Practices and Removal
- + Created version of Template that is in WORD 2007 format
- + New Forms
 - o Internet Use Approval Form
 - o Internet Access Request Form
 - o Updated forms
 - o Internet Usage Policy – Employee Acknowledgement (short form)
 - o Email Usage Policy – Employee Acknowledgement (short form)

Version 5.1

- + New section on Internet, email, and Electronic Communication
- + New forms
 - o Internet Usage Policy – Employee Acknowledgement
 - o Email Usage Policy – Employee Acknowledgement

Version 5.0

- + New section on Sensitive Information
- + New forms
- + Checklist For Separating Employees
- + Supervisor Checklist For Separating Employees

Version 4.1

- ✚ New section on Lost Equipment
- ✚ New section on Termination
- ✚ Deciding whether to fire
- ✚ Carrying out the fire decision
- ✚ New attached Excel spreadsheet internal controls check list for Sarbanes-Oxley section 404 compliance.

Version 4.0

- ✚ New section on Travel and Off-Site Meetings
- ✚ Updated Inspection Check List Form