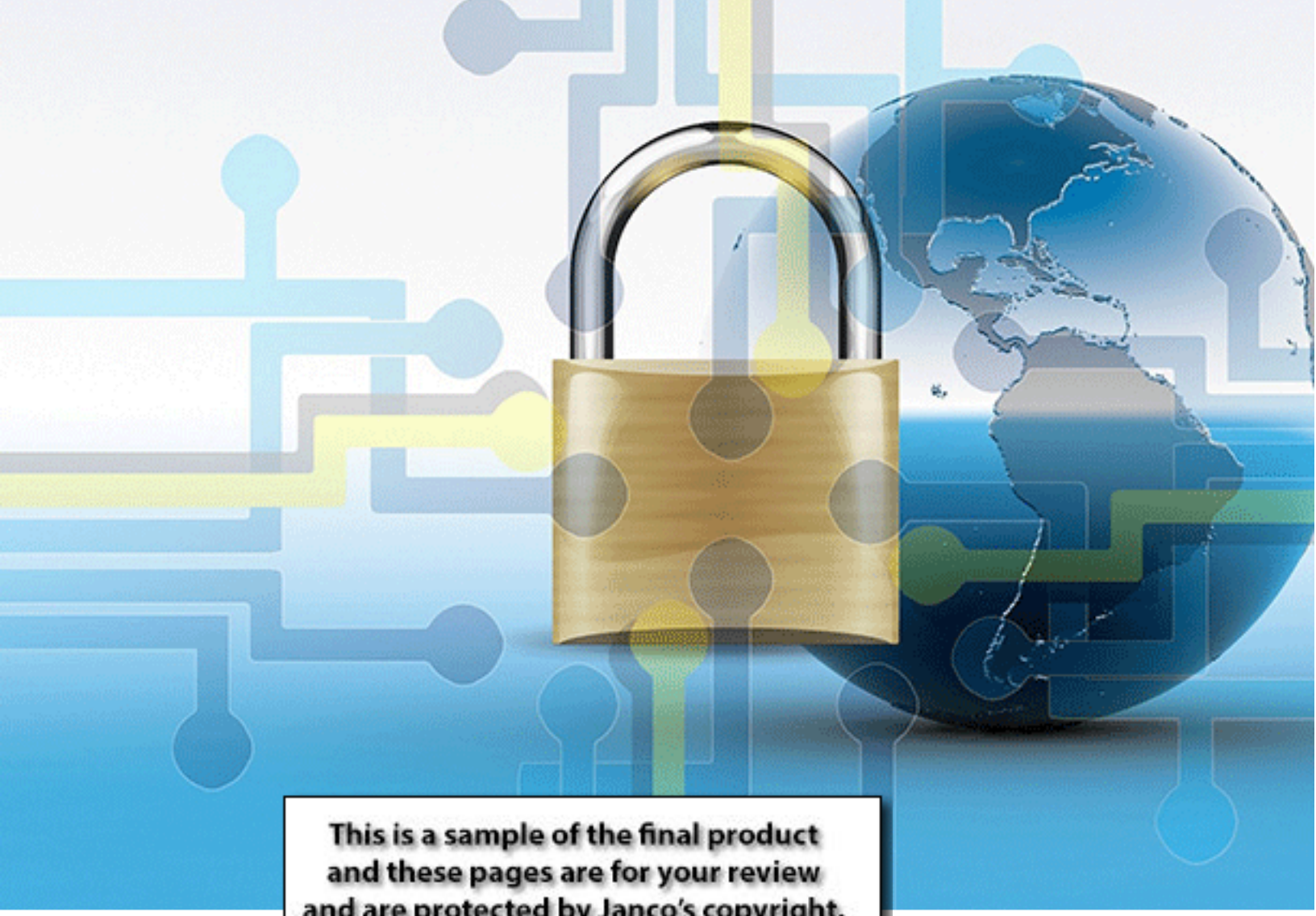
Compliance Management

Gold Edition

Jancoo Associates, Inc.



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

https://www.e-janco.com

Compliance Management

Janco Associates, Inc.

2022 Edition

Table of Contents

License Conditions 1
Table of Contents 2
Compliance Management 3
Compliance Requirements 4
Record Classification, Management, Retention, and Destruction 4
ISO Security Domains 5
ISO 27000 6
Governmental Mandates 12
California Consumer Privacy Act (CaCPA) 12
California SB 1386 Personal Information Privacy 14
COPPA 14
FCRA 14
FCTA 14
FISMA 15
FTC Information Safeguards 15
General Data Protection Regulation (GDPR) 16
Gramm-Leach-Bliley (Financial Services Modernization) 17
HIPAA 18
Massachusetts 201 CMR 17.00 Data Protection Requirements 23
Sarbanes-Oxley Act 23
State Security Breach Notification Laws 24
Implementation 26
Compliance Tools Purchase Options 29
Compliance Management Kit Versions 30
Silver Edition 30
Gold Edition 30
Platinum Edition 31
COBIT Edition 31
Version History 32

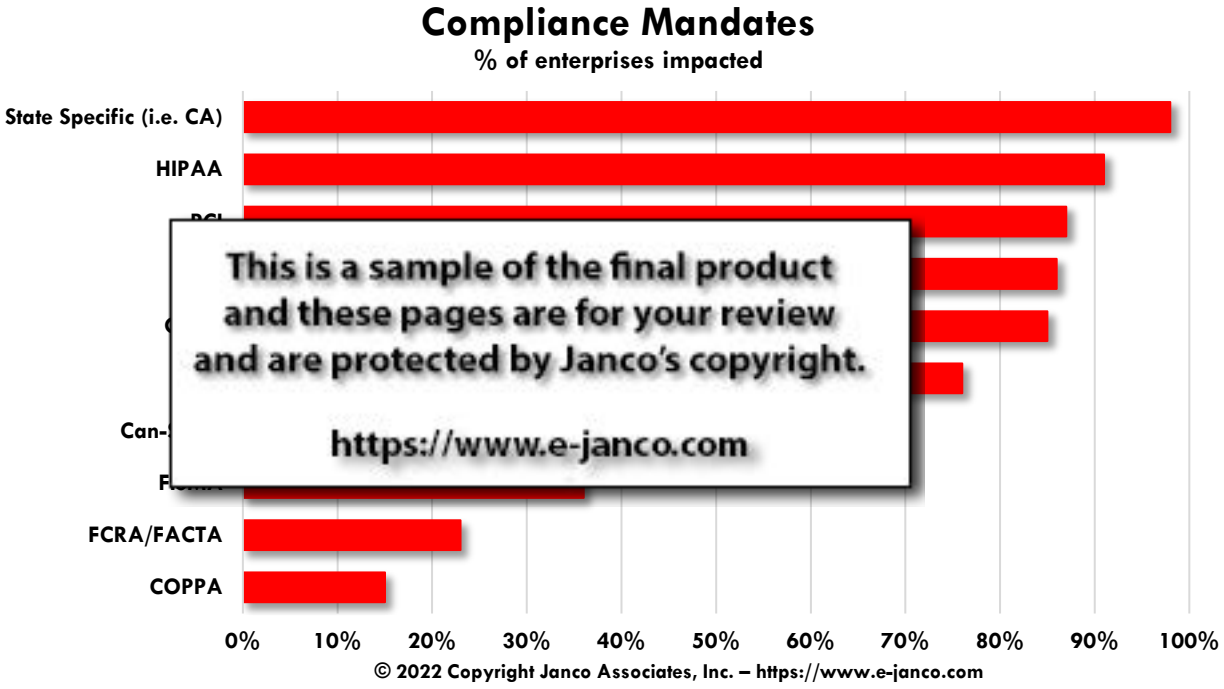
This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

https://www.e-janco.com

Compliance Management

Compliance is not an isolated IT project; it's an enterprise-wide endeavor that requires cooperation between business units and a deep understanding of the requirements, regulations, mandates and IT controls necessary for your industry and business. Compliance is as a business requirement that requires a cross-functional approach, involving people, processes and technology across the enterprise. Taking the steps necessary to understand, define and implement the appropriate IT controls and frameworks for your business will simplify compliance and reduce the costs and resources involved in completing compliance related tasks.

More small and mid-sized business are impacted by state-mandated (i.e. California, Massachusetts, New York, and others) than federal and SEC mandates.



Compliance Requirements

Record Classification, Management, Retention, and Destruction

The reality is that while regulatory compliance data, including Sarbanes-Oxley, ISO, financial or HIPAA medical, require long-term retention, many other common application data for almost every business, including those that do not fall under regulatory requirements, can benefit from - if not require - long–term data retention. The notion is to think beyond regulatory compliance. In other words, organizations of all sizes need and rely on information, both current and past.

A record is essentially any material that contains information about your company's plans, results, policies or performance. Anything about your company that can be represented with words or numbers can be considered a business record – and you are now expected to retain and manage every one of those records, for several years or even.

Record Classification Types	Retention Period
Accounts Payable Ledger	7 years
Accounts Payable Transactions	7 years
Accounts Receivable Ledger	7 years
Accounts Receivable Transactions	7 years
Accountant Audit Reports	Permanently
Bank Statements	7 years
Capital Stock and Bond records	Permanently
Inventory Records (products)	7 years
Insurance Records	Permanently
Invoices to Customers	5 years
Invoices from Vendors	5 years
Patents	Permanently
Payroll Records and Tax Returns	7 years
Purchase Orders	5 years
Safety Records	6 years
Time Cards and Reports	7 years
Training Manuals	Permanently
Union Agreements	Permanently

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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. – https://www.e-janco.com

Record Classification and Retention Periods

Janco (https://e-janco.com/recordmanagementpolicy.html) has a Record Classification, Management, Retention, and Destruction policy. It is a detail template which can be utilized on day one to create a records management process. Included with the policy are forms for establishing the record management retention and destruction schedule and a full job description with responsibilities for the Manager Records Administration.

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 also 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 [illegible] sed" and "influences the time an[illegible]tems, the world's largest ISO [illegible] the ISMS as "a systematic [illegible] remains secure. ISMS encompass[illegible]

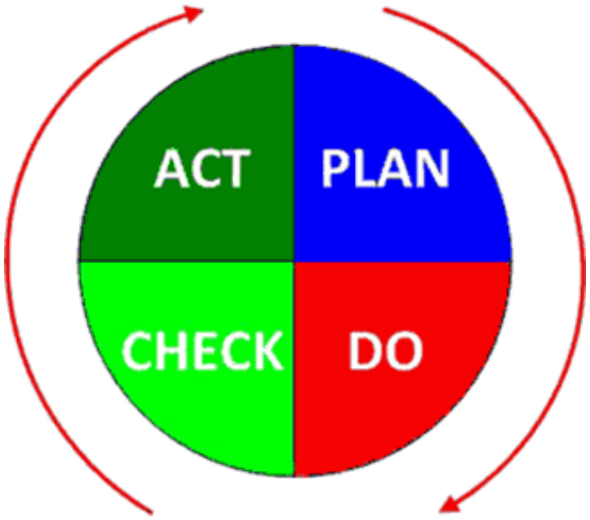
This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

https://www.e-janco.com

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

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.



© 2022 Copyright Janco Associates, Inc. – https://www.e-janco.com

ISO 27004 ering information security, s

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

https://www.e-janco.com

ISO 27005 d covering information security ri 7000 series, no firm dates hav SMS risk management process, i his is the ISO number assigned for an emerging standard for information security risk management.

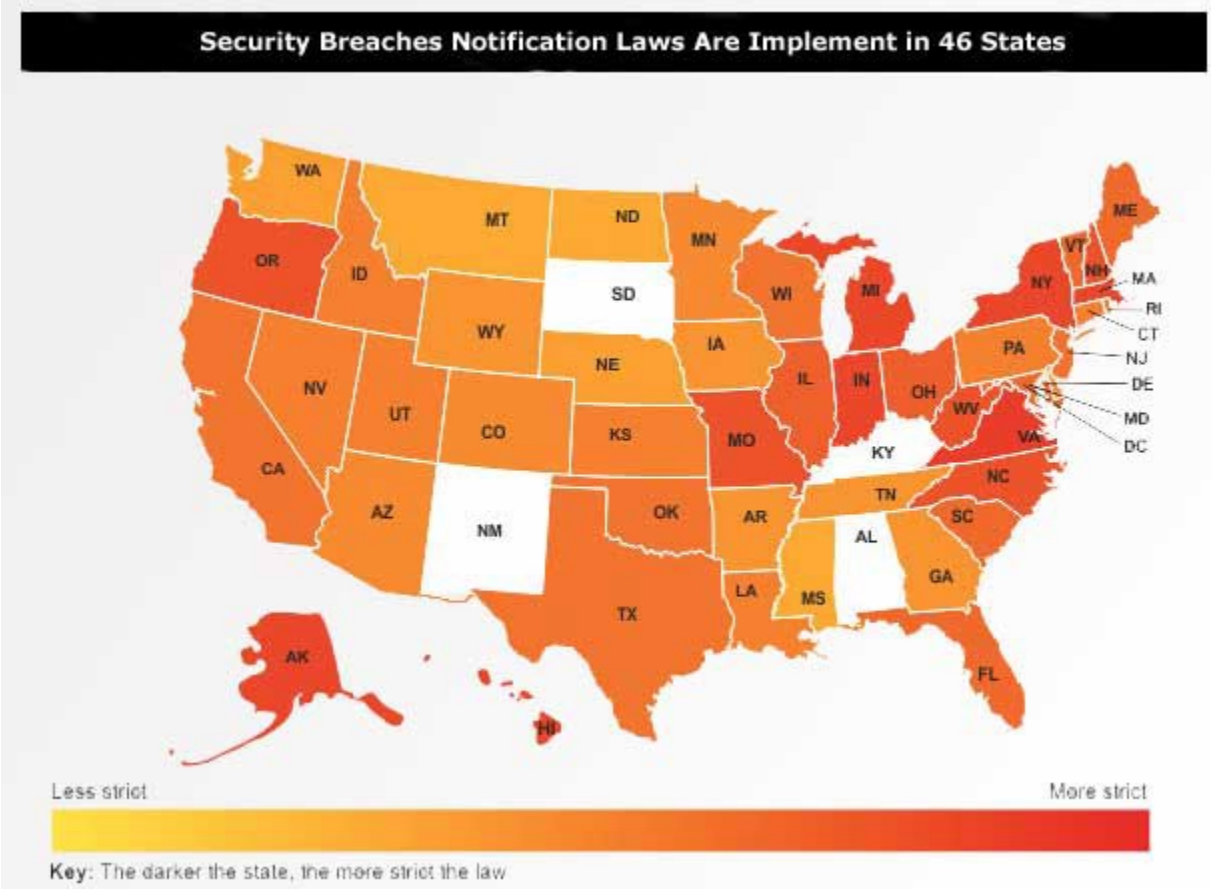
ISO 27006 - This standard offers guidelines for the accreditation of organizations that offer certification and registration with respect to ISMS.

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).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

State Security Breach Notification Laws

The landscape for CIOs and protection of personal information continues to become more complex as more states add breach notification laws. Currently, forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.



State Notification Requirements Table

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44-7501
	, 1798.82
Idaho	Idaho Stat. §§ 28-51-104 to 28-51-107
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.
Iowa	Iowa Code § 715C.1

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

https://www.e-janco.com

Compliance Tools Purchase Options

	COBIT	Compliance Management				Sarbanes Oxley			
		Std	Silver	Gold	Platinum	Std	Silver	Gold	Platinum
Compliance Management White Paper	X	X	X	X	X				
Record Management and Destruction Policy Template	X			X	X	X	X	X	X
PCI Audit Program	Included		X	X	X				
Compliance Management Job Descriptions	Included		X	X	X				
Security Audit Program	X		X	X	X				
Security Policies and Procedures Template	X				X				
Disaster Recovery Business Continuity Template	X					X	X	X	X
Practical Guide for IT Outsourcing	X					X	X	X	X
Business and IT Impact Questionnaire	X					X	X	X	X
Sensitive Information Policy	Included					X	X	X	X
Safety Manual Template						X	X	X	X
Threat & Vulnerability Assessment Tool	Included					X	X	X	X
Job Description Chief Security Officer	Included					X	X	X	X
Internet and Information Technology Position Descriptions HandiGuide	X						X	X	X
Internet and Information Technology 320 Position Descriptions								X	X
IT Service Management (ITSM) Service Oriented Architecture (SOA)	X								X
IT Infrastructure, Strategy, and Charter Template	X								
Service Level Agreement Policy Template with Sample Metrics	X								
Metrics for the Internet, Information Technology, and Service Management	X								
IT Salary Survey	X								

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

https://www.e-janco.com

Compliance Management Kit Versions

The Compliance Management Kit come is in 3 separate versions: Silver, Gold and Platinum. In addition, each version can be acquired as a standalone item or with 12 or 24 months of update service.

Silver Edition

- Compliance Management White Paper
- Security Audit Program - fully editable -- Comes in MS EXCEL and PDF formats -- Meets ISO 27001, 27002, Sarbanes-Oxley, PCI-DSS and HIPAA requirements -- Over 400 unique tasks divided into 11 areas of audit focus which are the divided into 39 separate task groupings including BYOD.
- PCI Audit Program - Word and PDF
- Compliance Management Job Description Bundle (25 key positions) - Word Format - fully editable and PDF - Chief Compliance Officer (CCO), Chief Data Officer, Chief Mobility Officer, Chief Security Officer, Data Protection Officer, Director Electronic Commerce, Director IT Management and Controls, Director Sarbanes-Oxley Compliance, Manager Blockchain Architecture, Manager BYOD Support, Manager Compliance, Manager E-Commerce, Manager Enterprise Architecture, Manager Internet Systems, Manager Record Administration, Manager Transaction Processing, Manager Video and Website Content, Manager Web Content, Manager Wireless Systems, PCI-DSS Administrator, System Administrators - Linux, System Administrators - Windows, System Administrators - UNIX, Webmaster, and Wi-Fi Network Administrator

Order at https://www.e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

Gold Edition

- Compliance Management White Paper
- Security Audit Program
- PCI Audit Program
- Compliance Management Job Description Bundle (25 key positions)
- Record Classification and Management Policy - Word - Policy which complies with mandated US, EU, and ISO requirements
- Privacy Compliance Policy that address the EU's GDPR and the latest California Consumer Privacy Act

Order at https://www.e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

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

https://www.e-janco.com

© 2022 Copy

Platinum Edition

- Compliance Management White Paper
- Security Audit Program
- PCI Audit Program
- Compliance Management Job Description Bundle (25 key positions)
- Record Classification and Management
- Privacy Compliance Policy that address the EU's GDPR and the latest California Consumer Privacy Act
- Security Manual Template - Word - 240 plus packed pages which are usable as is. Over 3,000 companies worldwide have chosen this as the basis for their best practices to meet mandated US, EU and ISO requirements

Order at https://www.e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

COBIT Edition

A much more robust version of the Compliance Kit with contains

- Compliance Management White Paper
- Record Classification Management Retention and Destruction Policy
- IT Infrastructure, Strategy, and Charter Template
- Disaster Recovery Business Continuity Template
- Practical Guide for IT Outsourcing
- Service Level Agreement Policy Template with Sample Metrics
- Metrics for the Internet, Information Technology, and Service Management
- IT Service Management (ITSM) Service Oriented Architecture (SOA)
- Internet and Information Technology Position Descriptions HandiGuide
- Security Policies and Procedures
- Security Audit Program
- Business and IT Impact Questionnaire
- IT Salary Survey

Order at https://www.e-janco.com/session/catalog_items.aspx?catalog=209&detail=1

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

https://www.e-janco.com

Version History

2022 Edition

- Updated meet latest mandated requirements
- Added Compliance Management Governance Purchase options table

2021 Edition

- Updated meet latest mandated requirements

Version 3.3

- Added details for CaCPA and GDPR
- Restructured all Governmental Mandates

Version 3.2

- Updated to meet the latest privacy and security mandates
- Added ePub version to the standard offering

Version 3.1

- Updated to included GDPR
- Updated to include CaCPA
- Updated all mandated requirements

Version 3.0

- Updated meet the latest ISO requirements
- Updated to reflect the US, EU, and state-mandated requirements
- Added sections on FISMA, FCRA, FACTA and COPPA compliance requirement

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

https://www.e-janco.com

Compliance Management

Job Descriptions HandiGuide®

Bundle

Table of Contents

- Chief Compliance Officer (CCO)
- Chief Data Officer
- Chief Mobility Officer
- Chief Security Officer
- Data Protection Officer
- Director Electronic Commerce
- Director IT Management and Controls
- Director Sarbanes-Oxley Compliance
- Manager Blockchain Architecture
- Manager BYOD Support
- Manager Compliance
- Manager E-Commerce
- Manager Enterprise Architecture
- Manager Internet Systems
- Manager Record Administration
- Manager Transaction Processing
- Manager Video and Website Content
- Manager Web Content
- Manager Wireless Systems
- PCI-DSS Administrator
- System Administrators - Linux
- System Administrators - Windows
- System Administrators - UNIX
- Webmaster
- Wi-Fi Network Administrator

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

https://www.e-janco.com

PCI Audit Program

2022

Janco Associates, Inc.

PCI Audit Program

Table of Contents

PCI Compliance Security Audit Program 2
Introduction 2
Policy - Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data 3
Policy – Record Management, Retention, and Disposition Policy 3
PCI DSS Applicability Information 4
Scope of Assessment for Compliance with PCI DSS Requirements 5
Instructions and Content for Report on Compliance 8
Revalidation of Open Items 9
Build and Maintain a Secure Network 10
Requirement 1: Install and maintain a firewall configuration to protect cardholder data 10
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. 16
Protect Cardholder Data 20
Requirement 3: Protect stored cardholder data 20
Requirement 4: Encrypt transmission of cardholder data across open, public networks 27
Maintain a Vulnerability Management Program 29
Requirement 5: Use and regularly update anti-virus software or programs 29
Requirement 6: Develop and maintain secure systems and applications 30
Implement Strong Access Control Measures 35
Requirement 7: Restrict access to cardholder data by business need-to-know 35
Requirement 8: Assign a unique ID to each person with computer access. 36
Requirement 9: Restrict physical access to cardholder data. 41
Regularly Monitor and Test Networks 45
Requirement 10: Track and monitor all access to network resources and cardholder data. 45
Requirement 11: Regularly test security systems and processes. 49
Maintain an Information Security Policy 52
Requirement 12: Maintain a policy that addresses information security for employees and contractors. 52
Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures) 59
Requirement A.1: Hosting providers protect cardholder data environment 59
Appendix B – Compensating Controls 62
Compensating Controls – General 62
Compensating Controls for Requirement 3.4 62
Appendix C: Compensating Controls Completed Example/Worksheet 63
Compensating Controls Worksheet 64
What's New 66

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com

PCI Compliance Security Audit Program

Introduction

The PCI Security Audit Procedures[1] are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS and the most recent set of privacy mandates – including GDPR.

This document contains the following:

- Introduction
- Policy – Sensitive Information
- Policy – Record Management, Retention, and Disposition
- PCI DSS Applicability Information
- The scope of Assessment for Compliance with PCI DSS Requirements
- Instructions and Content for *Report On Compliance*
- Revalidation of Open Items
- Security Audit Procedures
- Appendices
    - Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)
    - Appendix B: Compensating Controls
    - Appendix C: Compensating Controls Worksheet/Completed Example

With ever-increasing requirements placed by government legislatures and regulatory agencies, there are often competing and conflicting data retention/disposition requirements. For this reason, we have provided "draft" policies that can be utilized to create a customized "Sensitive Information Policy" and a "Record Management, Retention, and Disposition Policy."

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

https://www.e-janco.com

[1] Portions of this test program were extracted from the published PCI requirements and have been enhanced by Janco Associates, Inc. Note we are not attorneys and do not express any legal nor PCI standards opinion in this document. The use of this audit program should consult with their own legal and PCI compliance staff.

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com

PCI DSS Applicability Information

The following table illustrates commonly used elements of the cardholder and sensitive authentication data; whether the storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive but is presented to illustrate the different types of requirements that apply to each data element. At the same time compliance to Record Retention and Disposition standards (see https://www.e-janco.com/recordmanagementpolicy.html) needs to be coordinated with the PCI DSS requirements. A Sensitive Information policy (see https://www.e-janco.com/sensitive.htm) for the enterprise should be implemented.

	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

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

https://www.e-janco.com

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during business operations. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

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

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com

The scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all "system components." A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

A service provider or merchant may use a third-party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant services of the third party provider must be scrutinized either in:

1. Each of the third-party provider's clients' PCI audits; or
2. The third-party provider's PCI audit.

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or devices such as firewalls and routers)

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

https://www.e-janco.com

ement environment where more if some data repositories or sponsible for ensuring that all compliant with the PCI DSS

saction is accepted at a merchant station, supermarket, or other

- If there is no external access to the merchant location (by the Internet, Wi-Fi, Bluetooth, a virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded.

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall configuration standards that include the following:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	**1.1.1a** Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration			
	1.1.1b Verify th firewall.			
	1.1.1c Verify log			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify documents all c networks			
	1.1.2.b. Verify that the diagram is kept current			

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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com

What's New

2022 Edition

- Update to meet the latest requirements
- Updated graphics

Version 3.1

- Updated to meet the latest privacy and security requirements

Version 3.0

- Update to meet the latest requirements
- Updated graphics

Version 2.1

- Added Policy – Sensitive Information
- Updated tables

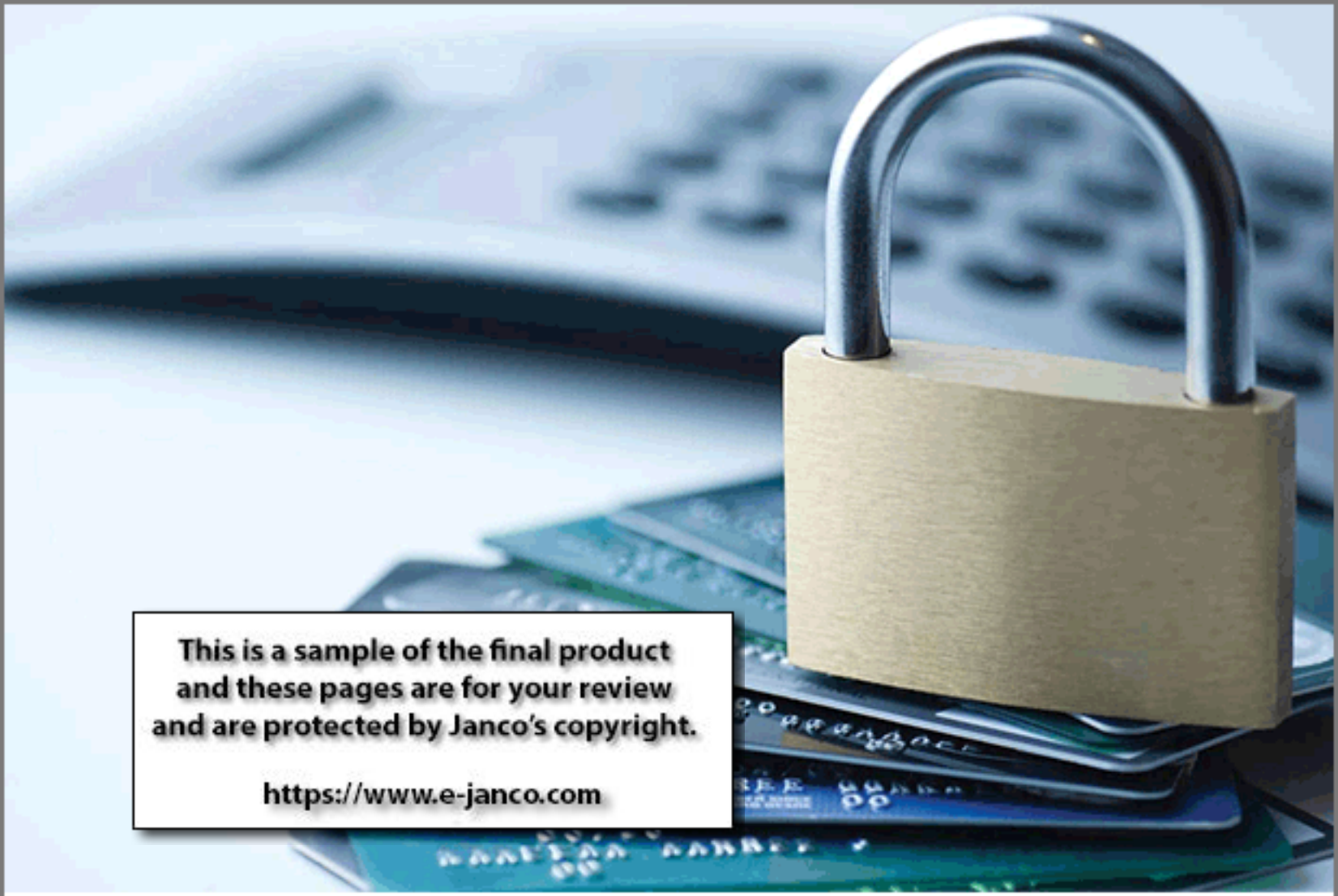
Version 2.0

- Added Policy – Record Management, Retention, and Disposition
- Modified style sheet and format to be CSS compliant
- Modified audit program to be compliant with the two added policies

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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. – www.e-janco.com



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

https://www.e-janco.com

Security Audit Program

Janco Associates, Inc.

2022 Edition

Table of Contents

Introduction
Security Audit Program Summary
Security Audit Program
Security Policy Management Objectives
Information Security Policy 1
Corporate Security Management Objectives
Internal Security Organization 2
External Use of the Enterprise Information 3
Organizational Asset Management Objectives
Responsibility for the Enterprise Assets 4
Information Classification System 4
Human Resource Security Management Objectives
Security Prior to Employment 5
Security During Employment 6
Security at Termination 7
Physical and Environmental Security Management Objectives
Secure Areas 8
Enterprise Equipment 8
BYOD 9
Communication and Operations Management Objectives
Procedures and Responsibilities 10
Third Party Service Delivery 10
System Planning Activities 10
Malicious and Mobile Code 11
Back-up Procedures 11
Computer Networks 11
Media 12
Exchange of Information 12
Electronic Commerce 13
Information Processing Facilities 13
Information Access Control Management Objectives
Access to Information 14
User Access Rights 14
Access Practices 15
Access to Network Services 15
Access to Operating Systems 16
Access to Applications 16
Mobile, Remote, and Work From Home 17
Systems Development and Maintenance Objectives
Information System Application Security 18
Application Processing Information 19
Cryptographic Controls 20
System Files 20
Development and Support Processes 20
Information Security Incident Management Objectives
Security Events and Weaknesses 21
Managing Security Incidents and Improvements 21
Disaster Recovery and Business Continuity Objectives
Disaster Recovery Plan / Business Continuity 22
Compliance Management Objectives
Mandated Security Requirements 23
Security Compliance Reviews 23
Security Audit Summary
Security Audit Program Completed Sample
Security Audit Program Summary Completed Sample

Ransomware, WFH, GDPR, CaCPA ISO, Cobit, HIPAA, and SOX Addressed

This audit program contains a list of tasks and and weights assigned to each task. The Excel sheet calculates the value of both positive and negative points. Based on the audit you place an "X" in the yes and/or no box and a value is automatically calculated. When the audit, which is on the worksheet 'Audit Program', is completed all of the results are them posted on the summary worksheet and graphic charts can be generated from those tables (see the attached sample).

The worksheets Audit Program Summary, Audit Program, and Audit Program Graphic are integrated - if you change the name on the on any of those three worksheets then the Audit Program Summary Sheet and Audit Program Graphic will not be generated correctly. We suggest that you make a copy of the entire excel file and delete the "Sample" worksheets.

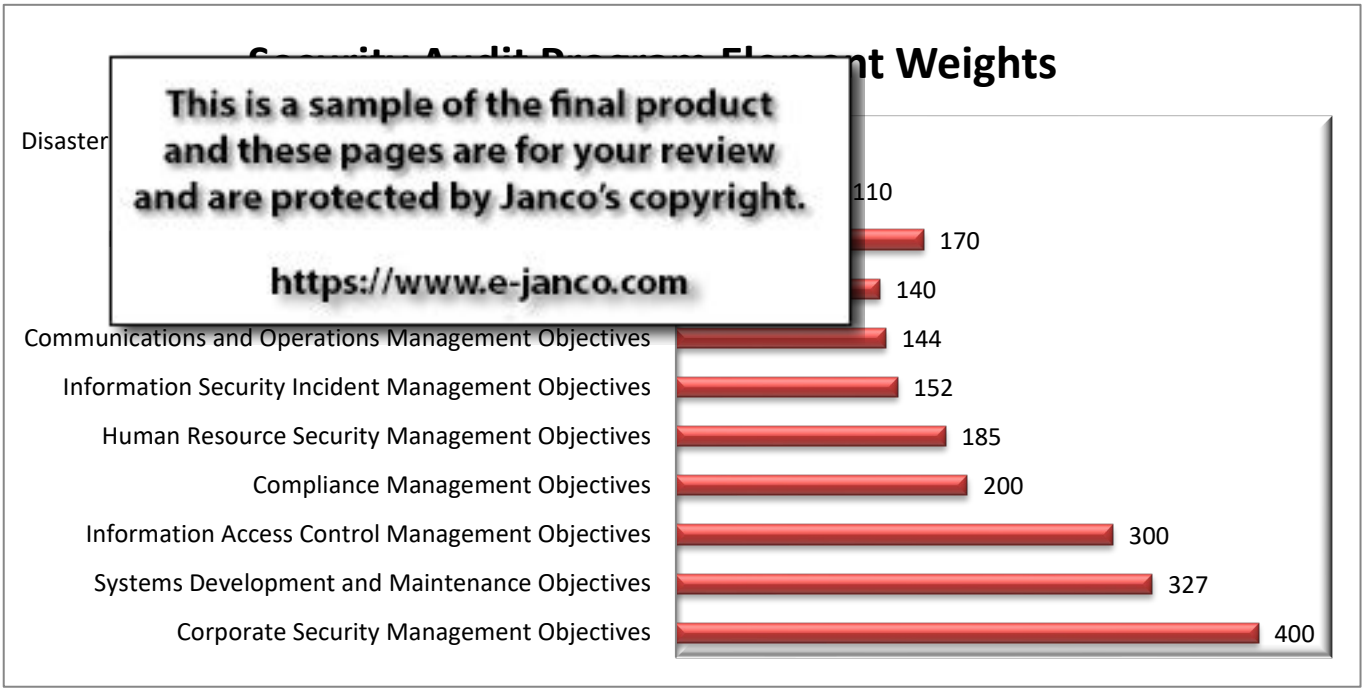
We have assigned weights to each element of the audit, you are free to updated to weights to what you think they should be. We assume no liability for the weight assignment and leave that up to the user. Our weights are only recommendations and should be considered as such.

The last three worksheets show a sample of the forms filled out with a set of summary graphic
We assume that the individual completing the form is knowledgeable in the use of Excel spreadsheets. Included with the excel spread sheet are a PDF version of the audit program that can be duplicated and used in the process. For ease you can fill out the survey manually and then transfer the data to the excel worksheet.

NOTE: An item can be marked both as a yes and a no, in which case it will impact both the positive and negative score.

This audit program is not to be re-sold or redistributed without the expressed WRITTEN permission of Janco Associates, Inc.

support@e-janco.com https://www.e-janco.com + 1 435 940-9300



© 2022 Janco Associates, Inc. Copyright - ALL RIGHT RESERVED

Security Audit Program

	Weight	Negative Score	Positive Score
	2,164	0	0
Security Policy Management Objectives	**110**	**0**	**0**
Information Security Policy	110	0	0
Corporate Security Management Objectives	**400**	**0**	**0**
Internal Security Organization	160	0	0
External Use of the Enterprise Information	240	0	0
Organizational Asset Management Objectives	**140**	**0**	**0**
Responsibility for the Enterprise Assets	70	0	0
Information Classification System	70	0	0
Human Resource Security Management Objectives	**185**	**0**	**0**
Security Prior to Employment	70	0	0
Security During Employment	60	0	0
Security at Termination	55	0	0
Physical and Environmental Security Management Objectives	**170**	**0**	**0**
Secure Areas	80	0	0
Enterprise Equipment	45	0	0
BYOD Equipment -- Number Devices _____	45	0	0
Communications and Operations Management Objectives	**144**	**0**	**0**
Procedures and Responsibilities	10	0	0
Third Party Service Delivery			
System Planning Activities			
Malicious and Mobile Code			
Back-up Procedures			
Computer Networks			
Media			
Exchange of Information			
Electronic Commerce			
Information Processing Facilities	14	0	0
Information Access Control Management Objectives	**300**	**0**	**0**
Access to information	55	0	0
User Access Rights	25	0	0
Access Practices	50	0	0
Access to Network Services	40	0	0
Access to Operating Systems	45	0	0
Access to Applications	50	0	0
Mobile, Remote, and Work From Home	35	0	0
Systems Development and Maintenance Objectives	**327**	**0**	**0**
Information System Application Security	84	0	0
Applications Processing Information	91	0	0
Cryptographic Controls	60	0	0
System Files	50	0	0
Development and Support Processes.	42	0	0
Information Security Incident Management Objectives	**152**	**0**	**0**
Security Events and Weaknesses	88	0	0
Managing Security Incidents and Improvements	64	0	0
Disaster Recovery Plan and Business Continuity Objectives	**36**	**0**	**0**
Disaster Recovery Plan / Business Continuity	36	0	0
Compliance Management Objectives	**200**	**0**	**0**
Mandated Security Requirements	80	0	0
Security Compliance Reviews	70	0	0
Information System Audits	50	0	0

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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

Security Audit Program

		Comment	Yes	No	Weight	Negative Score	Positive Score
Security Policy Management Objectives		**http://www.e-janco.com/Security.htm**			**110**	**0**	**0**
Information Security Policy					110	**0**	**0**
1.01	Validate that your enterprise has a security policy in place				**40**		
1.02	Validate that the policy provides clear direction for the enterprise's information security program.				**10**		
1.03	Validate that the policy shows that your management is committed to information security.				**10**		
1.04	Validate that management supports the enterprise's information security policy.				**10**		
1.05	Validate that the policy shows that your management is prepared to support an ongoing commitment to information security.				**10**		
1.06	Validate that the enterprise's information security policy is consistent with your business objectives.				**10**		
1.07	Validate that the enterprise's information security policy meets the enterprise's business requirements.				**10**		
1.08	Validate that the enterprise's information security policy complies with all relevant laws and regulations.				**10**		
1.09	Validate that Work From Home and remote users are following the enterprise's published security policies				**10**		
1.10	Validate that Busi Ransonware				**10**		

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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

Security Sample Audit Program (Sample Results)

	Weight	Negative Score	Positive Score
Security Policy Management Objectives	**110**	**10**	**110**
Information Security Policy	110	10	110
Corporate Security Management Objectives	**400**	**68**	**300**
Internal Security Organization	160	38	90
External Use of the Enterprise Information	240	30	210
Organizational Asset Management Objectives	**140**	**10**	**100**
Responsibility for the Enterprise Assets	70	10	50
Information Classification System	70	0	50
Human Resource Security Management Objectives	**185**	**40**	**145**
Security Prior to Employment	70	20	50
Security During Employment	60	0	60
Security at Termination	55	20	35
Physical and Environmental Security Management Objectives	**170**	**3**	**165**
Secure Areas	80	0	80
Enterprise Equipment	45	0	45
BYOD Equipment -- Number Devices 75	45	3	40
Communications and Operations Management Objectives	**144**	**30**	**112**
Procedures and Responsibilities	10	2	8
Third Party Service Delivery	12	4	8
System Planning Activities	6	0	6
Mal	26	0	26
Bac	6	0	6
Con	8	0	8
Mec	30	0	28
Exc	18	18	0
Elec	14	6	8
Info	14	0	14
Information Access Control Management Objectives	**300**	**40**	**260**
Access to information	55	0	55
User Access Rights	25	0	25
Access Practices	50	0	50
Access to Network Services	40	40	0
Access to Operating Systems	45	0	45
Access to Applications	50	0	50
Mobile, Remote, and Work From Home	35	0	35
Systems Development and Maintenance Objectives	**327**	**0**	**327**
Information System Application Security	84	0	84
Applications Processing Information	91	0	91
Cryptographic Controls	60	0	60
System Files	50	0	50
Development and Support Processes.	42	0	42
Information Security Incident Management Objectives	**152**	**88**	**64**
Security Events and Weaknesses	88	88	0
Managing Security Incidents and Improvements	64	0	64
Disaster Recovery Plan and Business Continuity Objectives	**36**	**0**	**36**
Disaster Recovery Plan / Business Continuity	36	0	36
Compliance Management Objectives	**200**	**0**	**200**
Mandated Security Requirements	80	0	80
Security Compliance Reviews	70	0	70
Information System Audits	50	0	50

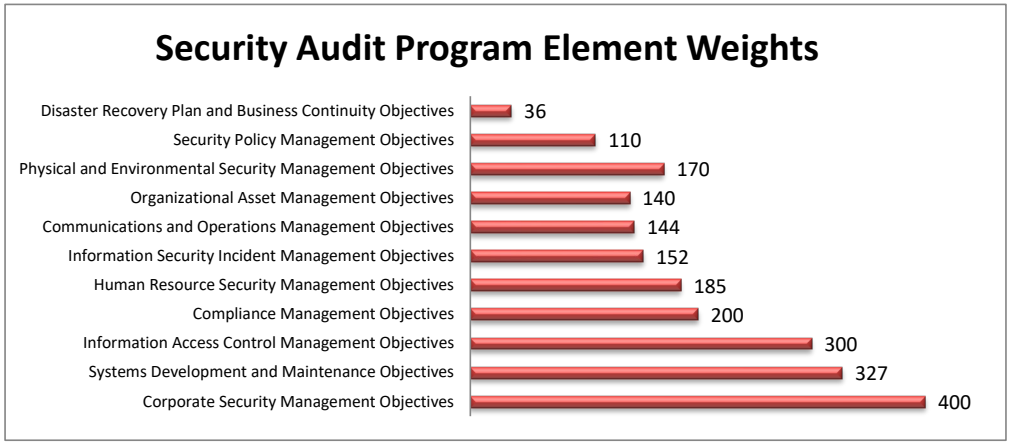
This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.

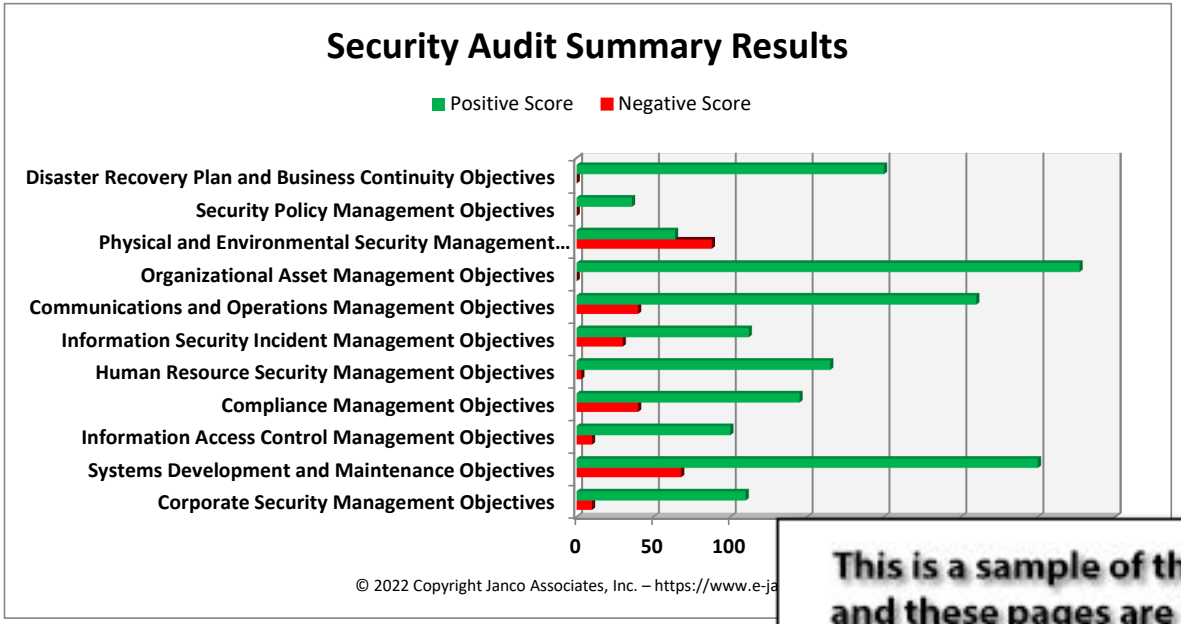
https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

Security Sample Audit Program Summary

	Weight	Negative Score	Positive Score
	2164	289	1819
Corporate Security Management Objectives	400	10	110
Systems Development and Maintenance Objectives	327	68	300
Information Access Control Management Objectives	300	10	100
Compliance Management Objectives	200	40	145
Human Resource Security Management Objectives	185	3	165
Information Security Incident Management Objectives	152	30	112
Communications and Operations Management Objectives	144	40	260
Organizational Asset Management Objectives	140	0	327
Physical and Environmental Security Management Objectives	170	88	64
Security Policy Management Objectives	110	0	36
Disaster Recovery Plan and Business Continuity Objectives	36	0	200





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

https://www.e-janco.com

© 2022 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

Privacy Compliance Policy

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

https://www.e-janco.com

Janco Associates

2021 Edition

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....24
Job Descriptions....24
Chief Security Officer....24
Data Protection Officer....24
Manager Compliance....24
Manager Security and Workstations....24
Security Architect....24
Privacy and Security Compliance Implementation Work Plan....25
What's New....27

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Privacy Compliance Policy – U.S. and EU Mandated Requirements

Overview

Mandated privacy requirements are designed to protect the individual's privacy from unwarranted invasion, to make sure that personal information in possession of an entity is properly used, and to prevent any potential misuse of personal information in the possession of that entity. This policy establishes the processes and procedures, and assigns responsibilities, for fulfilling mandated privacy requirements.

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

https://www.e-janco.com

The Chief Security Offi associated with information (data) tha des but is not limited to customer identificatio , credit card numbers, credit card expiration rs, ENTERPRISE proprietary data, and a

This policy applies to t and co-location providers and facilities regardless of the methods used to store and retrieve this information (e.g. online processing, outsourced to a third party, Internet, Intranet or swipe terminals).

All processing, storage and retrieval activities for this information must maintain the strict access control standards and the Chief Security Officer mandates these specific policies be followed.

Right to Privacy

Right to privacy has been defined in two major pieces of legislation – one for the EU (GDPR) and the other in the California Privacy act which was mandated in 2020

- The right to know what personal information is being collected about them.
- The right to know whether their personal information is sold or disclosed and to whom.
- The right to say no to the sale of personal information.
- The right to access their personal information.
- The right to equal service and price, even if they exercise their privacy rights.

The definition of the specifics of the legislation and policies necessary to comply follows. All individuals capturing, viewing or using consumer data need to follow the rules and guidelines to meet the Privacy Compliance Mandates.

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

California Consumer Privacy Act

Under the California Consumer Privacy Act, the following set of privacy requirements are mandated: and policies are to be followed.

Consumer's Right to Know Information that Has Been Captured

1. t collects a consumer's personal
   ic pieces of personal information the
2. all, at or before the point of collection,
   be collected and the purposes for which
   se shall not collect additional categories
   additional purposes without providing
3. An Enterprise shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.
4. An Enterprise that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. An Enterprise may provide personal information to a consumer at any time but shall not be required to provide personal information to a consumer more than twice in 12 months.
5. This section shall not require An Enterprise to retain any personal information collected for a single, one-time transaction if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.
   (1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.
   (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

GDPR

The General Data Protection Regulation (GDPR) sets specific compliance requirements on how your business does business with enterprises and individuals in the EU.

The EU requires personal data. Whether you rely on consent ngs to make sure you are GDPR compliant

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

https://www.e-janco.com

of collection
rget audience
t be hidden in small print.

- ❑ Give individuals control over their data. They should be able to decide whether to share their personal data with you or not.
- ❑ Under the GDPR principle of accountability, you should be able to demonstrate that you are compliant. This means recording the legal grounds for processing an individual's personal data.

Why Data is Captured

- ❑ To capture personal data the enterprise needs to demonstrate that they have a valid business or marketing reason to capture and retain data on an individual
- ❑ Validated that legitimate interests are the most appropriate lawful basis for processing
- ❑ Communicate how or why there is a need for an individual's personal data when it is collected
- ❑ Utilize a layered privacy notice/policy - A layered privacy notice puts the most important information up front and then there is a more detailed privacy policy underneath it
- ❑ Inform Individuals on what the plan is for their data when it is collected
- ❑ Allow individuals to "opt-out" of marketing
- ❑ Collect the minimum data necessary and delete records after use
    - Data needed for a suppression file can be kept.
    - Have a valid reason to process an individual's personal data using your legal legitimate interests. For example, an individual may have acquired a product, therefore, the business can market similar products to the customer

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Gramm-Leach-Bliley (Financial Services Modernization Act of 1999

Gramm-Leach-Bliley (GLBA) addresses both information security and privacy and holds ENTERPRISE management accountable to evaluate risks and implement controls to keep all information secure. Features of

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

https://www.e-janco.com

olicies related to
rd parties.

- Phone number
- Credit Card numbers
- Social Security Number
- Loan application information
- Credit history

- Customers need to be given the option to opt-out of having their private information disclosed.
- Notification should be:
  - At the beginning of the relationship and
  - At least annually to all customers

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

User/Customer Sensitive Information and Privacy Bill of Rights

Users and customers of the enterprise's systems and networks will have the following rights:

- Enterprise will provide Users/customers of the enterprise's systems a privacy policy regarding the data they collect.
- Users/customers of the enterprise's systems have the right to know what type of personally identifiable information is being collected and how long that personally
  related third party.
  enterprise or related
  connection with a
  dentifiable information
  from an enterprise or
  is reasonably believed to
  lt in identity theft or
  fraud.
- If a third party has been breached, the enterprise will report that to the enterprise's users/customers.
- Users/customers of the enterprise's systems will receive notice from the enterprise in the event of a data breach, by mail or e-mail, and without "unreasonable delay" (never later than 60 days after a breach, unless a criminal investigation is potentially affected.)
- Service providers that have obtained personally identifiable from the enterprise will send a notification regarding a data breach of protected information that is held by them, under mandated laws such as SOX, PCI, HIPPA, and other mandated requirements.
- Users/customers of the enterprise's systems will receive a general description of the actions taken by the enterprise to restore the security and confidentiality of the personally identifiable information involved in a data breach.
- Users/customers of the enterprise's systems will be provided at least 12 months of identity theft protection at the enterprise's expense.
- Enterprise will notify users/customers of a summary of the breach as victims of identity theft under the Fair Credit Reporting Act.

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Appendix

Forms

Attached forms which are in the subdirectory titled forms

Privacy Compliance Policy Acceptance Agreement

Job Descriptions

Attached job descriptions which are in the subdirectory titled Job Descriptions

Chief Security Officer

Data Protection Officer

Manager Compliance

Manager Security and Workstations

Security Architect

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

What's New

2021 Edition

- Updated to meet the latest compliance requirements
- Updated all the attached electronic form to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

2020 Edition

- Updated to meet the latest compliance requirements
- Updated all the attached electronic form to meet the most current version
- Updated all the attached job descriptions to meet the latest requirements

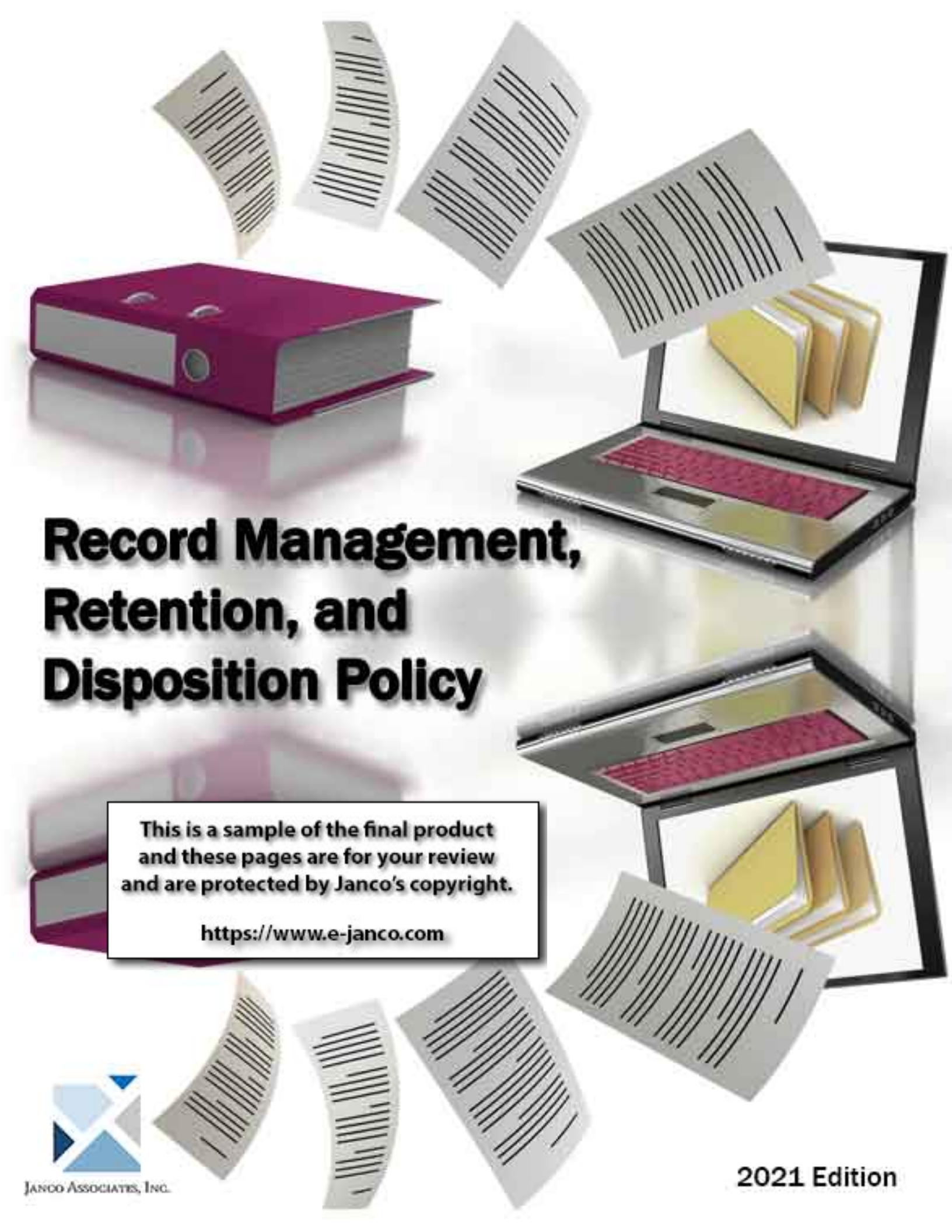
Version 2019

- Added Privacy and Security Compliance Implementation Work Plan
- Included electronic form as a stand-alone item
- Added detail job descriptions
    - Chief Security Officer
    - Data Protection Officer
    - Manager Compliance
    - Manager Security and Workstations
    - Security Architect

Version 2018

- Policy Released

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com



Record Management, Retention, and Disposition Policy

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

https://www.e-janco.com

Janco Associates, Inc.

2021 Edition

Table of Contents

Record Classification, Management, Retention and Disposition Policy Statement 2
Scope 3
Work From Home impact 3
What is Record Classification and Management 4
Regulatory Overview 5
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
Administrative Records
Facility Records
Financial Records
Sales Records
Computer and Information Security Records
Computer Operations and Technical Support
Data Administration
General Systems and Application Development
Network and Communication Services
User and Office Automation Support
Safety Records
Document Retention Periods 40
Federal Law Record Retention 41
Pennsylvania Record Retention 50
Massachusetts Record Retention 53
I-9 Retention 55
Version History 58

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Record Classification, Management, Retention and Disposition Policy Statement

Overview

Data and records that need to be retained are growing at a compound annual growth rate of 60% Data storage and information management costs need to keep up. As data volume and storage infrastructure grow, our company is tasked with meeting our operational service levels and cost containment objectives while also supporting corporate data retention, privacy, and eDiscovery obligations. Close cooperation between legal and IT is crucial to achieving this business, legal, and IT operational objectives.

Contrary to wh United States, regardless of size or industry g the Federal Rules of Civil Procedure (FRC

The FRCP is a b s district courts. The FRCP creates obligat , promptly, electronic information rel

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

https://www.e-janco.com

The executive management of ENTERPRISE has adopted guidelines to require that each ENTERPRISE unit institute record management, retention, and disposition procedures for the proper management of ENTERPRISE records. Executive management may, from time to time, amend the guidelines as appropriate or as required by law.

Such guidelines shall be consistent with applicable statutes governing the retention of original records and disposition of obsolete records, as well as with any contractual commitments or federal law or regulation which may apply. The guidelines provide for the proper maintenance and protection of archived records, and for the adoption of schedules for disposition of obsolete records, which schedules shall to the extent practicable given ENTERPRISE needs and requirements be consistent with requirements defined by executive management.

The words “records” means all books, papers, electronic files, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any employee of ENTERPRISE, executive office, department, board, commission, bureau, division or authority of ENTERPRISE.

Compliance with and implementation of the guidelines and any supplementary procedures is the responsibility of all ENTERPRISE employees.

Upon approval of the guidelines or any amendment thereto, the executive management shall forward the guidelines to all ENTERPRISE units. The executive management or its designees shall also establish specifications and timetables for the development of supplementary record classification, management, retention, and disposition procedures and data retention/disposition schedules for ENTERPRISE units. ENTERPRISE unit procedures must adhere to this policy and the published guidelines.

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

What is Record Classification and Management

The foundation of any good record management program is developing a consistent records classification system across the organization.

While there are many record classification systems, one recommended best practice is a three-tier classification based on business function, record class, and record type.

The first step toward developing such a records classification system is taking an inventory or a comprehensive and accurate listing of locations and contents of all records within the organization.

The second step is grou cord class, and record type:

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

https://www.e-janco.com

- ✓ ting, human resources,
- ✓ . For instance, two d accounts receivable.
- ✓ Record types are a further subdivision of record classes. For instance, the accounts payable record class can be further broken down into accounts payable aging reports, accounts payable distribution reports, cash disbursement reports, and other categories.

No matter which classification system is adopted, the selected system should address all records regardless of the media type.

The success of a records management program depends on the ease and efficiency of retrieval of the required data. The inability to retrieve the required data on a timely basis causes costly hold-ups, decreases organizational efficiency, degrades organizational quality, and even leads to litigations and fines.

The best practice in this regard is indexing all records, regardless of the media, in a systematic matter with multiple indexing heads. Possible indexing heads include subject matter based on content, subject matter based on context, record creator, intended recipient, date of creation, and others.

The indexing policy needs reinforcement through an access control policy and safeguards. The access policy should define:

- ✓ The extent of access to records for each employee.
- ✓ An authorization process that includes checks against the laid-down access policy before retrieval of records
- ✓ A means to record and track retrieval of records

A well-laid-out authorization and access policy help maintain confidentiality and prevents unauthorized disclosure or data theft.

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Primary Classification List of Records to Be Retained

There are hundreds of document types that may factor into an investigation or legal action. Such records are assumed to be searchable and quickly available upon request, under the rules of SOX. This even applies to less official types of records, like Emails or instant messages.

Some of the records types and retention time periods for physical and/or electronic records are:

Record Classification Types	Retention Period
Accounts Payable Ledger	7 years
Accounts Payable Transactions	7 years
Accounts Receivable Ledger	7 years
Accounts Receivable Transactions	7 years
Accountant Audit Reports	Permanently
Bank Statements	7 years
Capital Stock and Bond records	Permanently
Charts of Accounts	Permanently
Contracts and Leases	Permanently
Correspondence (legal)	Permanently
Deeds, Mortgages, Bills of Sale	Permanently
Patents	Permanently
Payroll Records and Tax Returns	7 years
Purchase Orders	5 years
Safety Records	6 years
Time Cards and Reports	7 years
Training Manuals	Permanently
Union Agreements	Permanently

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Record Classification by Device and Location

The record classification system considers the types of Device/media, location, approval for use, and limitations.

Device/Location	Approved	Limitations
Enterprise Device	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not use it for any personal or non-business-related purpose. All data that resides on enterprise devices is (and becomes) the property of the enterprise. All information is confidential and sensitive and should not be distributed outside of the enterprise with the expressed authorization of the enterprise.
Enterprise approved BYOD	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	vice to ed users. vice and on it at
Enterprise e-mail	Use the enterprise email account to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not conduct any personal business on the enterprise email account. Never open an unknown attachment or reply to anyone unknown to you.
Enterprise Cloud Storage	Use enterprise cloud storage to access enterprise information	Do not store personal information on enterprise cloud storage.
Personal Cloud Storage	For personal use only	Never store enterprise information on personal cloud storage

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Regulations and Industry Impact

Regulation	Industry Impacted	Retention Implications	Penalties
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			$250,000 & up to 10 years
Affordable Care Act			as they are set
FERPA	Education	Protects the privacy of student education records.	Can hold the Institution or individuals liable under other statutes or common law tort
Gramm-Leach-Bliley (GLB)	Financial Services	The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter	Fines up to $100,000 for each violation, officers, and directors can be fined up to $10,000 for each violation, and imprisonment for up to 5 years, a fine, or both

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

https://www.e-janco.com

Regulations and Industry Impact Table

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Job Descriptions

Two (2) full job descriptions are included with this policy template. They come separately in their directory.

Manager – Record Administrator

Manager WFH Support

Record Management Coordinator

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Forms

Twelve (12) Record Classification electronic forms are included with this policy template. They come separately in their directory.

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

Facility Records

Financial Records

Sales Records

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

https://www.e-janco.com

Computer and Information Security Records

Computer Operations and Technical Support

Data Administration

General Systems and Application Development

Network and Communication Services

User and Office Automation Support

Safety Records

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Document Retention Periods

	Years										
	1	2	3	4	5	6	7	8	9	10	PERM
Accounting Records											
Bank statements, reconciliations & deposit slips											
Dividend checks (canceled)											
Expense reports											
Monthly/interim financial statements											
Inventory count & costing sheets											
Fixed asset acquisition invoices (after disposal)											
Accounts payable ledgers (computer runs)											
Accounts receivable ledgers (computer runs)											
Cash books & cash register tapes											
Subsidiary ledgers											
Monthly trial balances											
Checks											
Payroll (individual time report & earnings records)											
Vouchers											
Audit reports											
General ledgers & journals											
Annual financial statement											
Income tax returns & work											
Payroll tax returns & W-2's											
Corporate Records											
Mortgages, notes & leases											
Bylaws, charter & minute b											
Checks (taxes, property & [illegible]											
Contracts & agreements (after termination)											
Copyrights, trademark & patent registrations											
Deeds & easements											
Partnership agreements or corporate documents											
Labor contracts											
Capital stock & bond records											
Patents											
Proxies											
Retirement & pension records											
Correspondence											
General											
License, traffic & purchase											
Production											
Legal											
Insurance											
Policies (after expiration)											
Accident reports											
Fire inspection reports											
Group disability records											
Safety reports											
Claims (after settlement)											

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

https://www.e-janco.com

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Version History

2021 Edition

- Updated for WFH impact on record retention requirements
- Added job description for Manager WFH Support
- Updated all included forms
- Updated all included job descriptions

2020 Edition

- Added materials on record classification
- Updated all the electronic forms
- Updated all of the attached job descriptions

Version 2.4

- Added materials on record classification
- Changed title to include Classification
- All the electronic forms were updated to facilitate the record classification process
- Update the included job descriptions

Version 2.3

- Restructured the policy to meet best practices standard
- Updated all electronic forms
- Updated all job descriptions
- Updated to meet the latest compliance mandates

Version 2.2

- Updated all of the electronic forms to meet the latest mandated, ISO, and EU requirements
- Reviewed record retention requirements - made adjustments as necessary
- Updated Job Descriptions

Version 2.1

- Added job description - Record Management Coordinator
- Added legal definitions
- Updated to meet the latest compliance requirements

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Version 2.0

- Restructured the entire procedure
- Added interviewee checklist for implementation of record management, retention, and disposition policy
- Add annual review process of record management, retention, and disposition policy
- Updated compliance requirements
- Updated all electronic forms

Version 1.7

- Updated Employer Record Retention Federal Requirements
- Updated for the Affordable Care Act
- Added Electronic Forms for Record Retention and Disposition Schedule
    - Personnel Records
    - Administrative Records
    - Facility Records
    - Financial Records
    - Sales Records
    - Computer and Information Security Records
    - Computer Operations and Technical Support
    - Data Administration
    - General Systems and Application Development
    - Network and Communication Services
    - User and Office Automation Support
    - Safety Records

Version 1.6

- Updated for latest I-9 record retention requirements
- Updated citations to include Lilly Ledbetter Fair Pay Act

Version 1.5

- Updated Citations for Federal Laws

Version 1.4

- Added Citations for Federal Laws

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com

Version 1.3

- Updated Regulations and Impact Section
- Added citations for Pennsylvania in Appendix
- Added citations for Massachusetts in Appendix

Version 1.2

- Updated Job Description Manager Record Administration
- Added Record Management Best Practices
- Updated Regulations and Impact Section

Version 1.1

- Expanded Email Retention and Destruction Section
- Added Document Retention and Destruction Table in Appendix

Version 1.0

- Policy Released

© 2021 Copyright Janco Associates, Inc. – www.e-janco.com