

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

<https://e-janco.com>

Policy

Sensitive Information



JANCO ASSOCIATES, INC.

2023 Edition



Table of Contents

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data	3
Overview	3
Policy	3
PCI	4
HIPAA	4
California Consumer Protection Act (CCPA)	5
General Data Protection Regulation (GDPR)	6
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999)	6
Massachusetts 201 CMR 17.00 Data Protection Requirements	7
User/Customer Sensitive Information and Privacy Bill of Rights	8
Secure Network Standards	9
Payment Card Industry Data Security Standard (PCI DSS)	9
Install and Maintain a Network Configuration Which Protects Data	13
Wireless & VPN	14
Modify Vendor Defaults	14
Protect Sensitive Data	15
Protect Encryption Keys, User IDs, and Passwords	16
Protect Development and Maintenance of Secure Systems and Applications	17
Manage User IDs to Meet Security Requirements	19
Restrict Physical Access to Secure Data Paper and Electronic Files	20
Regularly Monitor and Test Networks	21
Test Security Systems and Processes	22
Email Retention Compliance	23
Policy	23
Email to be printed	25
Regulations and Industry Impact	26
Keys to Email Archiving Compliance	26
Privacy Guidelines	27
Best Practices	28
Best Practices for Text Messaging of Sensitive Information	28
US government classification system	30
Appendix	33
Job Descriptions	34
• Chief Security Officer (CSO)	34
• Manager Data Security	34
• Security Architect	34
Forms	35
• Sensitive Information Policy Compliance Agreement	35
• Work From Home IT Checklist	35
HIPAA Audit Program Guide	36
What's New	41



Sensitive Information Policy

Credit Card, Social Security, Employee, and Customer Data

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data

Overview

Sensitive information is defined as information that is protected against unwarranted disclosure. Access to sensitive information is to be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues on personal privacy, or for proprietary considerations.

Information sensitivity is the control of access to information or knowledge that might result in the loss of an advantage or level of security if disclosed to others.

Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business, or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information. If an individual or an organization violates this policy, its standards, or procedures, there are subject to immediate termination or contract revocation without recourse.

Policy

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

<https://e-janco.com>

The Chief Security Officer or delegate must approve all processing activities at ENTERPRISE associated not limited to social security numbers, credit passwords, customer names, customer (i.e. California Personal ID number) that is ors, any governmental agency, or other body

pliers (including outsourcers), and co-

location providers and facilities regardless of the methods used to store and retrieve sensitive information (e.g. online processing, outsourced to a third party, Internet, Intranet, or swipe terminals).

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



Sensitive Information Policy

Credit Card, Social Security, Employee, and Customer Data

	<i>Data Element</i>	<i>Storage Permitted</i>	<i>Protection Required</i>	<i>PCI DSS Requirement 3.4</i>
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name*	Yes	Yes*	No
Sensitive Authentication Data**	EMV Authentication Data	No	No	No
	Full Cardholder Name	No	No	No
	Cardholder PIN	No	No	No

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

<https://e-janco.com>

* These data elements must be protected in a manner consistent with PCI DSS requirements for the 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 the business. 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).



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	Fin		
HIPAA		of the patient plus 2 years	& 10 years

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

<https://e-janco.com>

Regulations and Industry Impact Table

Keys to Email Archiving Compliance

Four objectives must be met. They are:

- ✚ **Discovery** - Information must be easy to access and consistently available to meet legal discovery challenges from regulatory committees.
- ✚ **Legibility** - Information must have the ability to be read today and in the future, regardless of technology. When selecting archiving technology, companies should look for solutions that are based on open systems, if their Email application should change. For example, if a company migrates from Microsoft Exchange to Lotus Notes, it must still be able to quickly access and read archived Emails.
- ✚ **Auditability** - An Email archiving solution must have the ability to allow third parties to review the information and validate that it is authentic.
- ✚ **Authenticity** - Information must meet all security requirements, account for alteration, and provide an audit trail from origin to disposition. An audit trail can track any changes made to an Email.



Sensitive Information Policy

Credit Card, Social Security, Employee, and Customer Data

Job Descriptions

The job descriptions listed below come as separate files in their directory

- Chief Security Officer (CSO)
- Manager Data Security
- 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://e-janco.com>



Sensitive Information Policy

Credit Card, Social Security, Employee, and Customer Data

Forms

The forms listed below come as separate files in their directory

- Sensitive Information Policy Compliance Agreement
- Work From Home IT Checklist

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

<https://e-janco.com>



What's New

2023 Edition

- ✚ Added 3 job descriptions
 - Chief Security Officer (CSO)
 - Manager Data Security
 - Security Architect
- ✚ Updated to meet ISO compliance requirements
- ✚ Updated all included forms

2022 Edition

- ✚ Major re-edit of the entire policy
- ✚ Updated to meet ISO compliance requirements
- ✚ Updated all included forms

2021 Edition

- ✚ Updated all included forms
- ✚ Updated to reflect WFH impact
- ✚ Add Work From Home IT Checklist

2020 Edition

- ✚ Updated to meet CCPA-mandated requirements
- ✚ Added section on CCPA definition and mandated requirements
- ✚ Update the Security Compliance Agreement Form to meet CCPA-mandated requirements

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

<https://e-janco.com>