

PolicySensitive Information



2023 Edition



Table of Contents

ensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data	
Overview	
Policy	
PCI	
HIPAA	
California Consumer Protection Act (CCPA)	
General Data Protection Regulation (GDPR)	
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999	
Massachusetts 201 CMR 17.00 Data Protection Requirements	
User/Customer Sensitive Information and Privacy Bill of Rights	
Secure Network Standards	
Payment Card Industry Data Security Standard (PCI DSS)	
Install and Maintain a Network Configuration Which Protects Data	
Wireless & VPN	
Modify Vendor Defaults	
Protect Sensitive Data Protect Encryption Keys, User IDs, and Passwords	
Protect Development and Maintenance of Secure Systems and Applications	
Manage User IDs to Meet Security Requirements	
Restrict Physical Access to Secure Data Paper and Electronic Files	
Regularly Monitor and Test Networks	
Test Security Systems and Processes	
Email Retention Compliance	2
Policy	2
Email to be printed	
Regulations and Industry Impact	
Keys to Email Archiving Compliance	2
Privacy Guidelines	2
Best Practices	2
Best Practices for Text Messaging of Sensitive Information	2
US government classification system	3
Appendix	3
Job Descriptions	3
Chief Security Officer (CSO)	3
Manager Data Security	
Security Architect	
Forms	3
Sensitive Information Policy Compliance Agreement	3
Work From Home IT Checklist	3
HIPAA Audit Program Guide	30
What's New	1



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

The Chief Security Officer or delegate must approve all processing activities at ENTERPRISE associated

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright. not limited to social security numbers, credit asswords, customer names, customer (i.e. California Personal ID number) that is ors, any governmental agency, or other body

https://e-janco.com

ppliers (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

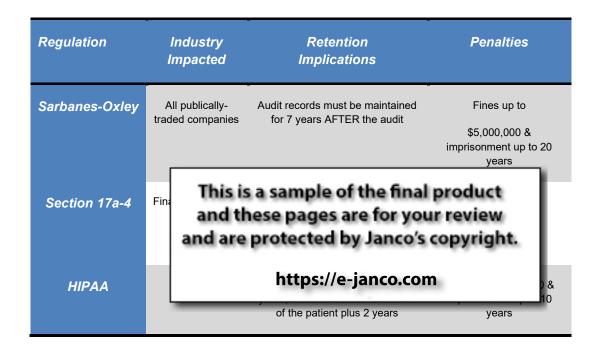
	Data Element	Storage Permitted	Protection Required	PCI DSS Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardbolder Name*	Voc	Voc*	No
Sensitive Authentication	This is a sa Ful and these and are prot	pages are	for your re	eview

this data or proper disclosure of a company's practices if consumer-related personal data is being collected during the business. PC 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



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.



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



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