Policy
Sensitive Information

Credit Card, Social Security, Employee, Customer Data

Janco Associates, Inc.

Version 3.5

Table of Contents

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 pertaining to personal privacy, or for proprietary considerations.

Information sensitivity is the control of access to information or knowledge that might result in 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 with sensitive information. This information includes but is not limited to social security numbers, credit card numbers, credit card expiration dates, security codes, passwords, customer names, customer numbers, ENTERPRISE proprietary data, and any other data (i.e. California Personal ID number) that is deemed to be confidential by ENTERPRISE, its external auditors, any governmental agency, or other body

including outsourcers) and co-
re and retrieve sensitive information
or swipe terminals).

n must maintain the strict access
ific policies be followed.

	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

* 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 the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

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

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	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

Keys to Email Archiving Compliance

There are four objectives that must be met. They are:

- **Discovery** - Information must be easy to access and consistently available in to meet
- in the future, mpanies should look eir Email application ft Exchange to Lotus Emails.
- allow third parties to review 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 Compliance Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

I hereby certify that I have reviewed ENTERPRISE's Secure Information policy and understand the policy, its standards, and procedures contained therein.

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 pertaining to personal privacy, or for proprietary considerations.

Information s ight result in loss of an advantage or

Loss, misuse, versely affect the privacy or welfare of l and foreign affairs of a nation depen tated that if I violate this policy, its standards or procedures, I am subject to immediate termination without recourse.

By signing this form, I affirm my willingness to abide by ENTERPRISE's security and sensitive information policies, procedures, and guidelines.

Signature _____ Date _____

What's New

Version 3.5

- Added General Data Protection Regulation (GDPR) requirements definition
- Updated electronic forms

Version3.4

- Updated to reflect latest compliance requirements'
- Updated to reflect lessons learned from recent business disruption events and known security breaches
- Included US government security classification system definition
- Added ePub (eReader) format to the standard offering

Version 3.3

- Updated electronic forms
- Added section on best practices for sensitive information text messaging

Version 3.2

- Added user/customer sensitive information and privacy Bill of Rights

Version 3.1

- Added an overview section to the policy including a definition of what sensitive information is.
- Updated electronic form
- Updated to meet latest mandated requirements

Version 3.0

- Added privacy guidelines section
- Added MS WORD electronic version of the Sensitive Information Policy Compliance Agreement
- Updated to comply with new mandated requirements
- .docx and .pdf formats support enhanced

Version 2.4

- Updated to comply with Gramm-Leach-Bliley
- Updated to comply with Massachusetts and California requirements

Version 2.3

- Updated General Policy Statement to Include references to PCI and HIPAA Requirements

Version 2.2

- Updated to CSS Stylesheet
- Modified to comply with Record Management, Retention, and Destruction Policy
- Update Email record retention compliance requirements

Version 2.1

- Payment Card Industry Data Security Standard (PCI DSS) Added
- Best Practices Added
- Wireless and VPN Added
- Added as a separate document PCI DSS Audit Program (extracted from PCI standards documentation with modifications)

Version 2.0

- HIPAA Audit Program Added
- Office 2007 version Added