Viterbo University

PCI-DSS Security Policy

Introduction

1. Policy Statement

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

2. Applicability and Availability

This policy applies to all employees. (12.1) Relevant sections of this policy apply to vendors, contractors, and business partners.

3. Policy Requirements

II. Adherence to standards

(2.2.a) Configuration standards must be maintained for applications, network components, critical servers, and wireless access points. These standards must be consistent with industry-accepted hardening standards as defined, for example, by SysAdmin Assessment Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS). [2.2.b should be captured in your system configuration standard; 2.2.c and 2.2.3.b should be covered in your procedure for new server set-up]

Configuration standards must include:

- (5.2) updating of anti-virus software and definitions
- (6.1.b) provision for installation of all relevant new security patches within 30 days
- (8.5.8.b) prohibition of group and shared passwords

III. Handling of Cardholder Data

(9.7) Distribution, maintenance, and storage of media containing cardholder data, must be controlled, including that distributed to individuals. (9.9) Procedures must include periodic media inventories in order to validate the effectiveness of these controls.

(3.1) Procedures for data retention and disposal must be maintained by each department and must include the following:

- legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data
- provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data
- coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, an audit process, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements
- (9.10) destruction of media when it is no longer needed for business or legal reasons as follows:
  - cross-cut shred, incinerate, or pulp hardcopy materials
  - purge, degauss, shred, or otherwise destroy electronic media such that data cannot be reconstructed

(3.3) Credit card numbers must be masked when displaying cardholder data. Those with a need to see full credit card numbers must request an exception to this policy using the exception process.

(4.2.b) Unencrypted Primary Account Numbers may not be sent via email

IV. Access to Cardholder Data

(7.1) Procedures for data control must be maintained by each department and must incorporate the following:

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignment of privileges is based on individual personnel's job classification and function
- Requirement for an authorization form signed by management that specifies required privileges
- Implementation of an automated access control system

V. Critical Employee-Facing Technologies

(12.3) For critical employee-facing technologies, departmental procedures shall require:

- (12.3.1) explicit management approval to use the devices
- (12.3.2) that all device use is authenticated with username and password or other authentication item (for example, token)
- (12.3.3) a list of all devices and personnel authorized to use the devices
- (12.3.4) labeling of devices with owner, contact information, and purpose
- (12.3.8) automatic disconnect of modem sessions after a specific period of inactivity
- (12.3.9) activation of modems used by vendors only when needed by vendors, with immediate deactivation after use

Departmental usage standards shall include:

- (12.3.5) acceptable uses for the technology
- (12.3.6) acceptable network locations for the technology
- (12.3.7) a list of company-approved products
- (12.3.10) prohibition of the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem
- (12.3.10) prohibition of use of cut-and-paste and print functions during remote access

VI. Roles and Responsibilities

Chief Security Officer (VP of Finance and Adminstration)

(12.5) Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- (12.5.1) creating and distributing security policies and procedures
- (12.5.2) monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- (12.5.3) (12.9) creating and distributing security incident response and escalation procedures that include:
- (12.9.1) roles, responsibilities, and communication
- (12.9.1) coverage and responses for all critical system components
- (12.9.1) notification, at a minimum, of credit card associations and acquirers
- (12.9.1) strategy for business continuity post compromise
- (12.9.1) reference or inclusion of incident response procedures from card associations
- (12.9.1) analysis of legal requirements for reporting compromises (for example, per California bill 1386)

- (12.9.2) annual testing
- (12.9.3, 12.9.5) designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
- (12.9.4) plans for periodic training
- (12.9.6) a process for evolving the incident response plan according to lessons learned and in response to industry developments
- (12.6; 12.6.1.a) maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)
- (10.6.a) review security logs at least daily and follow-up on exceptions
- (12.2.a) The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators

System and Application Administrators shall:

- (12.5.2) monitor and analyze security alerts and information and distribute to appropriate personnel
- (12.5.4) administer user accounts and manage authentication
- (12.5.5) monitor and control all access to data
- (12.10.1) maintain a list of connected entities
- (12.10.2) perform due diligence prior to connecting an entity, with supporting documentation
- (12.10.3, 12.4) verify that the entity is PCI-DSS compliant, with supporting documentation
- (12.10.4) establish a documented procedure for connecting and disconnecting entities
- (10.7.a) retain audit logs for at least one year

Department Heads

Department Heads (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- (12.6.1.b) facilitating participation upon hire and at least annually
- (12.6.2) ensuring that employees acknowledge in writing that they have read and understand the company's information security policy
- (12.7) screen potential employees to minimize the risk of attacks from internal sources

Internal Audit

Internal Audit (or equivalent) is responsible for executing a (12.1.2) risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

General Counsel

General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:

(12.8.1, 12.4) contracts require adherence to PCI-DSS by the service provider

(12.8.2, 12.4) contracts include acknowledgement or responsibility for the security of cardholder data by the service provider