Payment Card Data Standard

Purpose

This standard establishes a consistent and effective methodology for handling payment card data within the University to improve cardholder security and privacy and to meet compliance requirements

Scope

- Business activities which process, store or transmit cardholder data regardless of method or location
- Stored information containing cardholder data, regardless of age
- New services intending to process, store or transmit cardholder data
- Vendors who process, store, or transmit cardholder data on behalf of WPI.

Standard

Table of Contents

Definition of Cardholder Data

Cardholder data is the financial account information associated with credit or debit cards. This includes information about the cardholder, such as name and address, as well as the financial records themselves including the primary account numbers (PANs), verification codes, expiration dates, etc. Any information stored in printed form on the front or back of the card, as well as information embedded in the magnetic stripe or memory block inside the card is considered cardholder data.

All cardholder data at WPI, regardless of form, is classified as 'Restricted' according to the WPI Data Management Policy.

Roles and Responsibilities

WPI Office of Financial Services has overall responsibility for the safe handling of cardholder data for the University. This includes policy and standards development, overseeing vendor compliance status, as

well as the internal audit and compliance process.

WPI Information Technology is responsible to support the WPI Office of Financial Services by organizing and creating safe environments in which to process and handle cardholder data, maintaining a vulnerability management program as well as deploying and maintaining technical safeguards. This work is primarily organized through the Information Security group. This environment, including assigned terminals and/or dedicated PCs are the only methods allowed for processing credit card transactions. Use of any other method, device, or application must be approved by Information Technology.

Individual WPI Departments and employees are responsible for adhering to any approved policy and standards, and to notify the Information Security group if there is a concern with cardholder data handling or a breach of security. Department managers are responsible for ensuring that only individuals who have a business need receive access to such data.

Data Processing, Storage or Transmission

All business activities which process, store or transmit cardholder data must be approved for use by the WPI Office of Financial Services regardless of whether they are electronic or hardcopy processes. All aspects of security around the collection, handling and processing of cardholder data is deployed according to regulations and internal policies.

General

Information Management:

- All Primary Account Numbers (PANs) will be appropriately masked when displayed.
- Access to systems processing credit card information will be limited to only those authorized to perform credit processing via role-based authorizations.
- Appropriate access controls must be applied to all credit processing systems. Physical security around process devices will be maintained.
- Appropriate logs will be maintained.

Data Retention and Disposal:

- Departments are not allowed to store cardholder data after processing. All cardholder data used for processing is securely deleted or destroyed as soon as the transaction is complete.
- Paper data is destroyed by cross-cut shredding immediately after processing. All other media requiring destruction will be identified and processed appropriately.
- Properly-generated verification numbers, reports or receipts free of card holder data may be maintained for appropriate periods.

Electronic Data

Networking

- Systems processing cardholder data will reside on secured limited-access networks.
- Security standards for network devices will be maintained.
- Appropriate security technologies will be deployed in-line. These technologies include but are not limited to firewalls, intrusion detection systems, etc.
- Only approved, secure methods are used for the transmission of cardholder data regardless of its final destination.

System Security

- Appropriate security technologies will be deployed on the end-point systems. These technologies include but are not limited to host intrusion detection systems, anti-virus services, etc.

- All known vendor supplied defaults will be changed as appropriate.
- Systems will be 'hardened' by applying appropriate system policies.
- A system's service configuration will follow appropriate segmentation of duties.
- Remote access methods to a system will be limited.
- Systems will be kept patched and up-to-date.
- Encryption will be deployed to manage access to information when appropriate. Keys protecting the encryption routines will be deployed, utilized and protected.

Vulnerability Assessments

- All systems and networks are routinely scanned and audited using a variety of methods.

Hardcopy

Form Processing

- Hardcopy cardholder data will reside on a 'tear-off' portion of any form, which can be removed post-processing.
- Data waiting processing will reside in secure storage accessible only by those with designated responsibilities and proper training

Vendor Compliance

The WPI Office of Financial Services will review all vendors of WPI which process, store, or transmit cardholder data and ensure their compliance with any applicable compliance requirements on an annual basis. If a vendor is responsible for cardholder data on behalf of the University, a written agreement will be made for that vendor to acknowledge the responsibility of that data. All vendors must be compliant with any regulations, policies, and contractual obligations regarding cardholder data that apply to WPI or the vendor's jurisdiction appropriate to their role in processing, storing, or transmitting that data.

Awareness and Education

The WPI Office of Financial Services has developed appropriate awareness and education training materials to educate its employees on the proper handling of payment card data. This training is provided electronically via Cintas and is mandatory on an annual basis for all WPI personnel that process or handle credit card information. New employees with a business need will be provided the same Cintas training during their introductory period. The WPI Office of Financial Services is responsible for the records specifying who has completed the training. The material included in the Cintas PCI training is incorporated as part of this standard.

Incident Management

WPI Departments and employees who have a concern in the handling of payment card data or suspect a security breach should contact the Information Security Office immediately. The IT Incident Response Standard details the incident management plan to be implemented due to a breach.

Assessments and Monitoring

When a department wishes to add or change its existing business process in handling cardholder data, it must contact the WPI Office of Financial Services for an assessment. Finance will review the development plan, procedures list, and risks associated with handling data in the context of the change and will assist in meeting compliance as the new process is developed. As part of this assessment, Information Technology will also review any technical requirements and risks. Those aspects will be included in the schedule of changes. Projects of sufficient scope will require the project to be reviewed by University Governance. No system will be used to process cardholder data without approval by the WPI Office of Financial Services.

The WPI Office of Financial Services will periodically review department compliance to this standard. The WPI Information Technology office will review technical compliance to appropriate rules and regulations annually as well as at the direction of the Finance Office. All appropriate documentation will be kept on file to comply with financial audits of WPI and its financial partners.

Statement of Compliance

This document and any other related documents are intended to support and comply with PCI DSS.

February, 2016