WPI PCI Policy

1.0 Overview

WPI accepts credit cards as payment for a variety of goods and services. By accepting credit cards, WPI assumes significant risks with respect to protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed a set of financial and information technology standards, called Payment Card Information Data Security Standards (PCI-DSS), to protect credit cardholders' data.

This policy 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.

This policy addresses Payment Card Industry-Data Security Standards (PSI-DSS) that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment.

2.0 Applicability:

This policy pertains to all WPI departments and personnel that participate in credit and debit card processing. It requires them to have documented procedures that comply with the provisions and requirements of the PCI-DSS. The PCI-DSS is intended to mitigate the risks of identity theft and financial fraud associated with payment card use.

The policy covers the following specific areas contained in the PCI standards related to cardholder data:

- collecting
- processing
- transmitting
- storing
- disposing

All departments that participate in credit card processing must have documented procedures pertaining to the items noted above. The documents should be available for periodic review.

3.0 Definitions:

- Cardholder data (CHD) – Any personally-identifiable data associated with a cardholder. Such data include account number, expiration date, name, social security number, Card Validation Code, Card Verification Value, Card Identification Number, or Card member ID. All cardholder data at WPI, regardless of form, is classified as 'Restricted Use' according to WPI's *Data Classification and Usage Policy*.
- PCI-DSS - Payment Card Industry Data Security Standards
- Merchant – Organization that collects payments by credit or debit card (i.e., the University or one of its departments)

4.0 Policy

Credit Card Acceptance and Processing

- In the course of doing business at WPI, it may be necessary for a department to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards at the University is done on a case by case basis and coordinated through Office of Financial Services.

- Any department accepting credit cards on behalf of the University must designate an individual within the department who will have primary authority and responsibility within that department for maintaining required procedures for credit card transactions.

- Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account.

Credit Card Data Security Policy

Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

- Cardholder data collected are restricted only to those users who need the data to perform their jobs. Each department must maintain a current list of employees with

access and review the list annually, or when there is a change in staff, to ensure that the list reflects the most current access needed and granted.

- Cardholder data, whether collected on paper or electronically, are protected against unauthorized access.
- All equipment used to collect data is secured against unauthorized use in accordance with the PCI-DSS.
- Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data.
- Individual departments are held responsible for PCI compliance for all departmental procedures, applications, point of sale devices and departmentally administered servers that process, store or transmit cardholder data. The Chief Information Security Officer will work with departments that process credit cards to ensure that the departments are PCI compliant.
- Prohibition against using non-secure channels such as email, Instant Messaging (IM), or Social Media to transmit CHD or as a method to supply such information; and, in the event that this prohibited use does occur, disposal and/or reporting as outlined in WPI's *Data Retention and Destruction Policy* and *Data Breach Procedure*.
- If a fax machine is regularly used to transmit credit card information to a merchant department, provision of a stand-alone machine with no other purpose and with physical security commensurate with the security provided to paper records that contain CHD; and disposal of faxed CHD according to the requirements outlined in *Data Retention and Destruction Policy*
- No database, electronic file, or other electronic repository of information will store full credit/debit card numbers, the full contents of any track from the magnetic stripe, or the card-validation code.
- WPI issued computers and portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: desktops, laptops, compact disks, floppy disks, USB flash drives, personal smart phones, tablets and portable external hard drives.
- Cardholder data in paper form should be retained for three months or less for reconciliation purposes and destroyed immediately following the required retention period. A regular schedule of deleting or destroying data should be established in the

department to ensure that no cardholder data is kept beyond the record retention requirements. Paper documents should be shredded in a cross-cut shredder. Electronic data should be sanitized with an electronic shredding tool sponsored by the University.

Data Retention and Destruction

- CHD in paper form must be stored in a physically secure location, for no more than three months for reconciliation purposes, or in very limited situations by donor request for longer periods, and destroyed immediately following the required retention period.
- The department is responsible for maintaining a regular schedule for deleting or destroying CHD to ensure none is kept beyond applicable record retention requirements as per the Records Retention and Destruction Policy.
- Paper documents containing CHD must be shredded in a cross-cut shredder.
- Electronic data must be sanitized with an electronic shredding tool sponsored by the University.

Responding to a Security Breach

The *WPI Data Breach Procedure* outlines the requisite actions to take in the event of a breach. Specific to a PCI-DSS breach or suspected breach of security, the department or unit must immediately execute each of the relevant steps below:

- Follow the contact procedures in WPI's *Data Breach Procedure* document.
- Document every action taken from the point of suspected breach forward, preserving any logs or electronic evidence available.
- If the affected machine is a desktop or laptop, disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the computer uses a wireless connection, disconnect from the wireless network. If the affected device is a server, contact the Chief Information Security Officer and ask to have the device disconnected from the Network. DO NOT turn the device off or reboot to preserve evidence of the breach. Leave the device powered on and disconnected from the network.
- Notify the Chief Information Security Officer and the department head of the department experiencing the breach. Email (from an unaffected system) may be used for

initial contact but the details of the breach should not be disclosed in email correspondence.

- Prevent any further access to or alteration of the compromised system(s). (i.e. do not log on to the machine and/or change passwords; do not run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.
- If warranted, WPI will invoke further actions from the *Data Breach Procedure*.

5.0 WPI PCI Roles

PCI CONTACT PERSON:
Michelle Pickett
Senior Treasury Analyst
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-5470
Fax: (508) 831-5715

CHIEF INFORMATION SECURITY OFFICER (CISO):
John Schwartz
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-6868
Fax: (508) 831-5483

6.0 Responsibilities for Compliance

PCI-DSS compliance at WPI is a joint effort among all departments associated with collecting payments to WPI by means of credit and debit cards. The Senior Treasury Analyst and the CISO are responsible for PCI compliance. These offices work jointly to ensure that the departments who process CHD are PCI-compliant. They also attest to merchant bank(s) regarding the University's PCI compliance. Individual departments are responsible for the compliance of their personnel, procedures, applications, point-of-sale devices, and departmentally administered systems that process or transmit CHD. Departmental representatives will be required to

participate in periodic PCI compliance audits and implement any procedural or system changes that may be required by the Senior Treasury Analyst and the CISO upon recommendation by the EVP, CIO, internal auditors, or external auditors.

7.0 Enforcement

Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment card collection capability for affected departments.

Any person that violates any of the measures found in this policy will be subject to the same disciplinary actions outlined in WPI's Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

8.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 09/26/2018.

Policy Reviewed Annually By: John Schwartz (CISO)

Related University Policies:

Data Classification and Usage Policy
Records Retention and Destruction Policy
WPI Data Breach Procedure

Additional Information:
https://www.pcisecuritystandards.org

Last Modified: 10/30/19