The University of Scranton

Division of Information Technology

Executive Sponsor:
Associate Vice President for Information Technology/CIO

Credit Card Handling Security Standard

Responsible Office:
Information Security

Issued: 4/2013
Revised: 1/2022
Reviewed: 1/2022

I. Standard Statement

The University and all departments that process credit or debit card information must comply with the Payment Card Industry Data Security Standards (PCI DSS). This includes the acquiring, accepting, capturing, storing, processing or transmitting of credit or debit card data, in both electronic and non-electronic formats.

II. Reason for Standard

This document is intended to provide guidance regarding the processing of charges and credits on credit and/or debit cards. These standards are intended to protect against exposure and possible theft of account and personal cardholder information that has been provided to the University of Scranton and ensure compliance with industry regulations.

III. Entities Affected By This Standard

Any department, auxiliary organization, entity or individual that in any way accepts, captures, stores, processes or transmits credit or debit card information, using campus information assets, (both electronic and non-electronic), or uses third-party service providers to do this for you, is governed by this Information Security Standard.

IV. Website Address for this Standard

https://www.scranton.edu/information-technology/policies.shtml

V. Related Documents, Forms, and Tools

VI. Contacts

For policy clarification and interpretation, contact the Associate Vice President for Information Technology/CIO at 570-941-6185. For legal advice and interpretation of law, please contact the Office of General Counsel at 570-941-6213.

VII. Definitions

PCI-DSS: Payment Card Industry Data Security Standards, a proprietary information security standard for organizations that handle branded credit cards from the major card schemes.

VIII. Responsibilities

Information Security Office (ISO)

- ISO will coordinate organizational compliance and documentation.

- ISO will advise organizations on appropriate documentation of compliance and procedures to ensure alignment with PCI-DSS requirements.

- ISO will maintain a central list of devices used for the processing of cardholder data. The ISO will periodically inspect devices for tampering.

Department Responsibilities

- Each department which conducts credit card transactions under an assigned Merchant ID (MID) shall designate an individual to serve as the PCI DSS contact for the department, responsible for completing the requisite documentation and ensuring the department is compliant with PCI-DSS.

- The department contact shall compile and maintain a list of users in their department who interact with cardholder data. The department contact shall notify the ISO when changes to this list occur.

- The department contact shall notify the ISO of any changes to hardware, software or services used to process cardholder data prior to the changes being implemented.

- Communicate procedures to staff – The department head in units effected by this standard should communicate the department credit card security handling procedures to staff and ensure that the “Credit Card Handlers and Processors Responsibilities” section of this standard is followed by all personnel involved in credit card transactions.

- Prevent unauthorized access to cardholder data and secure the data – The department head should establish procedures to prevent access to cardholder data in physical or electronic form. Hard copy or media containing credit card information should be stored in a locked drawer or office, and password protection should be used on computers.

- Restrict access based on a business need-to-know – Access to physical or electronic cardholder data should be restricted to individuals whose job requires access.

- Assign a unique ID to each person with computer access – User names and passwords may not be shared.

- Transmitting credit card information by e-mail or fax – Full or partial credit card numbers and three or four digit validation codes (usually on the back of credit cards) may not be faxed or emailed.

- Never store electronically the CVV, CVV2 validation code, or PIN number - Departments must not store the three or four digit CVV or CVV2 validation code from the credit card or the personal identification number (PIN).

- Background Checks – consistent with the University's new hire process, a background check is performed on all new hires. This practice has been in place prior to the development of these Credit Card Handling Security Standards. If adverse information is discovered through the background check process, the action taken will be directed by the background check policy and will be subject to the adverse action process. The decision to allow a new hire to begin employment, or an existing employee to continue employment, will be made in accordance with the University's background check policy.

- All individuals who were employed prior to the University adopting the mandatory background check policy are not required to have a background check retroactively. For sake of establishing a cutoff date, all employees who began employment prior to the inception of this standard are not required to have a background check to work in areas where credit card processing is required.

- Mask 12 of the 16 digits of the credit card number - Terminals and computers must mask all but the first 6 digits and/or the last 4 digits of the credit card number (masking all digits but the last 4 is standard practice on campus).

- Using imprint machines – Imprint machines need special handling as they display the full 16 digit credit card number on the customer copy. Departments should not use imprint machines to process credit card payments unless personnel have been authorized to do so, and processes exist to securely store and dispose of the information.

- Report Security Incidents to the Information Security Office - If staff or faculty know or suspect that credit card information has been exposed, stolen, or misused; this incident must be reported immediately to Information Security Office. The report must not disclose by fax or e-mail credit card numbers, 3- or 4-digit validation codes, or PINs.

IX. Procedures

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS is a set of comprehensive requirements for enhancing credit card data security. The standards were developed by the PCI Security Standards Council, and a single violation of any of the requirements can trigger an overall non-compliant status. Each non-compliant incident may result in steep fines, suspension and revocation of card processing privileges. Although the primary focus of the PCI DSS is on web-based sales and processing credit card information via the Internet, there are other processes that allow systems to be Internet accessible which may expose cardholder information.

Payment Methods, Hardware, and Services

PCI DSS requires the merchant to inventory, document, and secure all payment methods used to process card transactions. In order to ensure PCI DSS compliance, all hardware, software, payment accessories (e.g. card swipe hardware, receipt printer), mobile applications, and related third-party services (e.g. payment processors) must be reviewed and authorized by the Information Security Office (ISO) prior to implementation. Any modifications to existing payment methods should also be reviewed.

Storing Credit and Debit Card Holder Data

Card holder data is any personally identifiable data associated with a cardholder. This can be an account number, expiration date, name, address, social security number, or Card Verification Value (CVV or CVV2).

Storage of credit cardholder data refers to both electronic (databases, spreadsheets, etc.) and non-electronic (faxes, imprint machine slips, hand written forms, etc.) data. The best way to be in compliance with PCI DSS is by **NOT** storing credit card holder data if there is no business need to do so.

Credit Card Handlers and Processors Responsibilities

Staff or faculty with access to credit or debit card holder data must not:

- Acquire or disclose any cardholder's credit card information without the cardholder's consent including but not limited to the full or partial 16-digit credit card number, 3- or 4-digit validation code (usually on the back of credit cards), or PINs (personal identification numbers).

- Transmit or request any credit card information by e-mail or fax. If someone e-mails their data, you should make them aware that, for their own safety, they should not do this again. The email or fax should be destroyed as soon as possible.

- Electronically store or record any credit card information in any electronic format (Excel files, databases, e-mail, etc.) unless you have been authorized to do so by their department head and the Information Security Office.

- Request, record, or store any of the magnetic stripe data or the credit card confirmation code (3 digit on the back of many cards and 4 digits on the front of American Express).

- Share a computer password if you have access to a computer with credit card information

Staff or faculty with access to credit or debit card holder data should:

- Change a vendor-supplied or default password if you have access to a computer with credit card information.

- Password protect your computer if you have access to a computer with credit card information.

- Store all non-electronic, physical documents, or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.

- Store all electronic files containing credit card information on a secured server, or as encrypted or password protected files.

- Report immediately a credit card security incident to your department head and the Information Security Office if you know or suspect credit card information has been exposed, stolen, or misused.

- Destroy all media used for credit cards when retired from use. Properly shred all hard copies prior to disposal.

Compliance

Violations of any part of this policy will subject violators to the regular disciplinary processes and procedures of the University that apply to students, faculty, staff, graduate teaching assistants, work study students, and all third parties.

X. Appendix