The University of Scranton

Division of Information Technology

Executive Sponsor:
Associate Vice President for Information Technology/CIO

/ŇJŜŘλű /Ⅰ·ŇJŘ ⅠⅠ·yŘfλyƎ {ŜŎdzŇJλűè {ű Ⅰ·yŘⅠ·ŇJŘ

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

Background Checks ς consistent with ΰΚŜ ¦ yϏØŜℕăλΰèΩă yŜø ΚΛℕŜ LJℕ2ŎŜăăΣ I· ōI·Ŏ]Ξℕ2dzyŘ 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 accordanŎŜ øλΰK ΰΚŜ ¦ yϏØŜℕăλΰèΩă ōI·Ŏ]Ξℕ2dzyŘ ŎΚŜŎ] LJ2fλŎè¢

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 ς 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