NSCS Information Security Standard 11: Payment Card Data Protection

The Payment Card Information (PCI) data security standards (DSS) apply to all entities that store, process or transmit cardholder data. NSCS departments that accept credit card payments must process those payments in a manner compliant with PCI-DSS standards in addition to other regulatory requirements. All use of credit cards for NSCS business must be approved in writing by both the CISO and Vice-President for Administration and Finance (VPAF).

- Each College is required to comply with the PCI-DSS SAQs appropriate to the equipment and services being used at the College.
- Each College shall maintain procedures to ensure compliance with the appropriate PCI-DSS SAQs
- In general, these operating principles shall be followed:
    - When possible, use credit card processing technologies that remove transport networks and equipment from PCI scope, such as P2PE.
    - When a P2PE compliant POS card reader cannot be used, either network segmentation or analog phone lines must be utilized to limit PCI scope as narrowly as possible.
    - Use third party processors for payments which require no payment card data to be received by the NSCS. This means that all departments that accept credit cards over the Internet must redirect all such payment card submissions to a third-party website.
    - Vendors on NSCS premises are responsible for their own POS card readers, transport mechanisms and PCI-DSS compliance. In the case of P2PE capable devices, NSCS may provide vendors with transport to reduce costs.
    - Storage of credit card information on computers or other electronic media by NSCS employees is strictly prohibited.
    - E-mailing credit card information is strictly prohibited.
    - Receipts should only print the last four digits of the card, be shredded when no longer needed, and protected as PII.
    - The credit card expiration date is not to be included on the receipt.
    - Receipt printouts are to be minimized, but if needed, will be stored with appropriate physical safeguards, including storage in locked cabinets with access restricted to those with legitimate business need.

The Vice-President for Administration and Finance or their designee, one at each college, collaborates with the CISO to manage a compliance program as an extension of managing merchant identification numbers. Participation in the PCI compliance program is mandatory for all organizations within NSCS that process payment cards. Failure to fully participate in the program may result in an organization's Merchant ID being revoked. The following outlines the major responsibilities for PCI-DSS compliance.

11.1 Shared Responsibilities

The VPAF and CISO are responsible for:

- Coordinating merchant accounts with the System Office and regulatory agencies. A merchant account is a type of bank account that allows businesses to accept payments by debit or credit cards.
- Establishing and maintaining contractual relationships with third-party providers involved with credit card processing.
- Approving any Point of Sale (POS) device or system to be used within the college and maintaining an inventory including make, model and serial number.
- Ensuring that payment card processing logs are maintained.
- Defining the methods of transacting online payments on behalf of the college.
- Engaging a PCI Qualified Security Assessor. See Information Security Standard 6: *Vulnerability and Penetration Testing* for specific scanning requirements.
- Maintaining an inventory of all individuals who process credit card transactions.
- Ensuring annual PCI training and education for everyone approved to process payment cards. Such training will include instruction on how to detect skimming.

11.2 VPAF Responsibilities

- Ensuring that each payment card unit is inspected monthly for tampering and maintaining an inspection log.
- Suspension or termination of the ability to process payment cards if an individual or department fails to comply with this policy or the PCI Standard.

11.3 CISO Responsibilities

- Ensuring network segmentation configurations and other technical safeguards are in place.
- Assisting in evaluating and approving all POS devices used at the college.
- The CISO ensures the configuration of the IT infrastructure to limit the applicability of PCI-DSS requirements to the infrastructure including approving and implementing network segmentation configurations performed in compliance with this policy and the PCI-DSS Standard.
- Assisting employees with PCI-DSS compliant implementations.
- Working with the VPAF to ensure appropriate vulnerability scanning of NSCS systems that transmit, generate or otherwise access payment card information.
- Initiating investigations relating to PCI-DSS security incidents.

- Performing monitoring and reviews of the computer infrastructure to ensure that security features are in place and are adequate to protect payment card data.

11.4 Self-Assessment Questionnaires

Colleges will complete periodic self-assessment questionnaires (SAQs) as needed to ensure compliance.

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/26/2019: Third review by SOISO
Oct/1/2019: Fourth review by SOISO