North Shore Community College

Institutional Data Security Policy - Credit Card Processing (PCI)

As an authorized merchant of the credit card payment industry, North Shore Community College will comply with the Payment Card Industry Data Security Standards when accepting, processing, transmitting and storing credit card information to protect our constituent's credit card information and ensure compliance with PCI regulatory requirements.

This policy applies to all North Shore Community College departments and affiliated units, employees, consultants, and other service providers. This policy is applicable to any unit that accepts, processes, transmits, or handles cardholder information in a physical or electronic format. All electronic devices at North Shore Community College involved in processing payment card data are subject to the PCI Data Security Standards. This includes servers which store payment card transactions, workstations which are used to enter payment card information into a central system, and any computers or credit/debit card swipe devices through which the payment card information is transmitted

All transactions that involve the transfer of credit card information must be performed on systems approved by the Chief Information Officer or his designee and will include a compliance and security review. Any specialized servers that have been approved for this activity must be housed and maintained behind a firewall configuration established by the College and approved by the CIO, and must be administered in accordance with the requirements of PCI policies.

Departments involved with the acceptance or processing of credit card information for payment of goods and services must design adequate controls and processes that meet these specified guidelines:

1. Merchant accounts must be requested through the Comptroller's office.
2. The Comptroller's Office and Chief Information Officer review and recommend purchases of software and/or equipment related to credit card processing before entering into any contracts. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device).
3. Departments must comply with the Payment Card Industry Data Security Standard. (refer to PCI Data Security Standard – for level 3 merchant).
4. E-mail is not to be used to obtain or transmit complete credit card information.
5. Under no circumstances can documents containing credit card holder information leave the college premises.
6. Establish written departmental procedures for safeguarding cardholder information and secure storage of data. Procedures must address telephone, over the counter, mail, internet and fax communications.
7. Documents containing credit card holder information must not be transmitted or received via unmonitored fax machines.
8. Documents containing credit card holder information must be transported in locked bags between campuses according to the transport of receipts procedure, to ensure transport is authorized and securely delivered.
9. Documents containing credit card holder information must be transported between departments on the same campus in person, and authorized by the department manager.
10. Sensitive cardholder data [i.e., full account number, card type, expiration, and card-validation code (three-digit or four-digit value printed on the front or back of the card) must not be stored in any College system, credit card terminals, personal computer, lap top computer, external storage devices or e-mail account.

Revised July 15, 2010

11. Credit card terminals should be programmed to mask all but the last four digits of the credit card account number. Complete credit card numbers must not be printed or written on either the merchant or customer copy of any receipts
12. All documentation containing credit card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with access limited to individuals who are authorized to handle credit card information. Processing of paper should be done as soon as possible. In the event that a document containing credit card information must be stored, all credit card information should be blacked out.
13. Credit card transaction receipts will be retained according to the College's approved business requirement retention policy of no longer than18 months in a secure (locked) environment. If there is no underlying business purpose to retain this data it should be destroyed at the earliest feasible time frame. All media used for credit cards must be destroyed when retired from use. All hardcopy must be crosscut shredded prior to disposal.
14. NSCC employees involved with credit card data must review this policy and agree not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent, and to follow all PCI standards. Supervisors are responsible for reviewing these policies with their employees at least annually or as needed to ensure compliance.
15. Require all personnel involved in credit card handling to attend PCI security training in conjunction with their job duties and PCI audits. Security training is the responsibility of both the SFS and Bookstore departments and much of it takes place as part of job training.
16. The Human Resource Department notifies Information Systems of changes to employment status due to termination or resignation, or other changes in status.
17. As outlined in the College's Internal Control Plan segregation of duties will be implemented whenever possible with appropriate supervisory review and oversight.
18. Only authorized employees will have access to credit card information based on their business function. A unique ID will be provided to each person and unique passwords required. These accounts require a written request from the manager/supervisor to the appropriate department for granting of any query and/or processing access.
19. NSCC does not use vendor-supplied system, application or administrator passwords.
20. Contractually require all third parties with access to cardholder data to adhere to PCI security requirements and provide proof of PCI certification to the merchant department.
21. Any suspected or identified breach should be reported immediately to the Business area supervisor who will then communicate with the Vice President responsible for that component and VP for Administration for immediate and appropriate action in accordance with Major Security Incident Policy (reference).

Violations of this policy may result in disciplinary action, up to and including dismissal, as well as civil liability and/or criminal prosecution.

This document is approved by the Executive Cabinet (President and VPs) and supported by the Vice President for Administration and Finance who established a committee comprised of cross component units to collaborate on PII/PCI DSS requirements, review existing College business practices involving credit card processes and to make recommendations for process change if needed to ensure compliance with PII/PCI DSS. The committee includes, Dean of Student Financial Services, Coordinator of Student Accounts, Chief Information Officer, Director of Applications, Comptroller, Asst. to Comptroller, Asst. VP for Budget and Planning, Bookstore Accountant.