62.31 Payment Card Industry Compliance Policy — POLICY

1.0 PURPOSE

1.1 The purpose of this policy is to establish guidelines for processing credit card payments to ensure compliance with Payment Card Industry Data Security Standards (PCI-DSS).

1.2 PCI-DSS defines the security requirements for transferring, handling and storing credit card information. Adhering to these standards will provide reasonable assurance that sensitive cardholder data received by NSCC during the processing of credit card payments is protected to the greatest extent possible.

2.0 SCOPE

1.1 This policy applies to all NSCC employees who are involved in accepting or processing credit card payments and pertains to all credit card transactions processed by NSCC.

3.0 DEFINITIONS

3.1	**Cardholder data**	is credit card information that can be compromised including the primary account number used with any of the following: expiration date, cardholder name or Card Verification Value code.
3.2	**Card Verification Value (CVV)**	is the 3 or 4 digit code that is typically located on the back of the credit card. For American Express cards, the code is a 4 digit unembossed number printed above the card number on the face of the credit card. This code is used to assist in the verification of the legitimacy of the credit card.
3.3	**Payment Card Industry (PCI)**	is the security-council founded by the major credit card providers
3.4	**Payment Card Industry Data Security Standards (PCI-DSS)**	are the standards developed by the PCI Security Standards Council. These standards govern the transferring, handling and storing of credit card information to ensure protection against fraud and unauthorized access.
3.5	**Point-of-sale (POS) terminals**	are used to process debit and credit transactions.
3.6	**Primary account number (PAN)**	is the 14 or 16 digit numeric code located on the front of the credit card. This number is used to identify the individual account holder.
3.7	**Quality Assurance (QA) recording system**	is any system that uses audio or voice recordings, typically in call centers, as a means of assessing the quality of service provided.
3.8	**Quality Security Assessor (QSA)**	is certified by the PCI Security Standards Council to conduct audits to ascertain an organization's level of compliance with PCI-DSS.

4.0 POLICY

4.1 Accepted Payment Channels

NSCC can accept credit card payments via telephone, mail, in-person or online.

a. In-Person Payments, Mail and Telephone Payments

i. Cardholder data manually recorded via mail, telephone or in-person transactions should only be retained for as long as it is required for business purposes. While cardholder data is retained, it must be stored in a locked area where access is restricted to staff who are authorized to process credit card transactions.

ii. Manually recording cardholder data during in-person transactions is not permitted unless the point-of-sale terminal is unavailable at the time the payment is submitted. Whenever possible, credit card payments should be completed using the point-of-sale terminal when customers are present using a chip card if available.

b. Email Payments

i. Cardholder data must never be sent or accepted via email. If information is received in this manner, the sender must be informed that NSCC does not accept payment information via email and will not process the payment until it is submitted through an accepted payment channel. All cardholder data must be deleted prior to sending the email response.

ii. After the email response has been sent, the email must be deleted as per the guidelines outlined in the Payment Card Industry Compliance Procedures.

c. Fax Payments

Cardholder data must never be sent or accepted via fax. If information is received in this manner, the sender must be informed that NSCC does not accept payments via fax and will not process the payment until it is submitted through an accepted payment channel.

d. Online Payments

All online payments must be processed using a PCI-compliant third party service provider that has been approved by the Director, Financial Services.

4.2 Storage Restrictions

a. Any manually recorded cardholder data that contains the cardholder's credit card number, expiry date and CVV code must be shredded or placed in the designated confidential shred receptacles immediately after the credit card payment has been processed. Redacting cardholder data is not sufficient when disposing of cardholder data.

b. Cardholder data will not be stored electronically in any format on a local computer, server, tablet, smartphone or on any removable storage devices such as USB keys, CDs or DVDs. This includes Excel and Word files.

c. The CVV code must never be stored under any circumstances after the transaction has been authorized. Paper documents where the CVV code has been recorded must be shredded or placed in a designated confidential shred receptacle immediately after the payment has been processed.

d. Multifunction machines must be set up by the vendor to ensure that faxed information is not retained in memory at any time. The vendor must provide a letter certifying that this set up has been completed on all NSCC multifunction machines.

e. Cardholder data must never be included in voicemail messages.

f. Cardholder data must never be recorded while using a QA recording system. If a QA recording system is being used, the recording must be suspended whenever cardholder data is discussed.

4.3 Distribution and Transmission of Cardholder Data

a. Documents containing credit card information must not be sent via interdepartmental mail between campuses or between departments within the same location.

b. Credit card payments received via mail, in-person or by telephone must be processed by the Campus and/or Central Office department that receives the payment information. Credit card information must be destroyed immediately after the credit card payment has been processed. Any related documents that need to be sent to a different campus or department must not contain any credit card information.

c. Any refund requests sent to Central Finance must not contain any cardholder data. The refund request should be sent Central Finance with a note that the refund is to be made to a credit card. Central Finance will contact the initiating Campus or Central Office department via telephone to obtain the credit card information required to process the refund.

d. Credit card information must never be photocopied or scanned using a photocopier or multifunction device.

4.4 Training and Awareness Program

a. Employees with work responsibilities that include accepting, storing, transmitting and/or processing credit card transactions, are required complete an Payment Card Industry Compliance Training Program on an annual basis.

b. Annually, employees must sign a certificate indicating that they have completed the required Payment Card Industry Compliance Training Program and have read and understood the Payment Card Industry Compliance Policy and Procedure documents.

4.5 Annual PCI Certification

NSCC will undergo an audit by a qualified QSA on an annual basis to obtain the required PCI-DSS compliance certification.

4.6 Policy Review

This policy will be reviewed annually to ensure its continued effectiveness in addressing PCI-DSS requirements. Updates will be done as required to reflect all changes to PCI standards or changes to the CDE.

5.0 POLICY SUPPORTS

Payment Card Industry Compliance Procedures (under development)