Procedure

Procedure Name	***Handling of Cardholder Data***		
Procedure #	IT 1.3	Parent Policy	IT 1.0
Policy Owner	Vice President, Administration	Effective Date	May 14, 2018
Procedure Owner	AVP Information and Technology Services, AVP Finance and Corporate Services	Next Review Date	April 27, 2027
Approved by	AVP Information and Technology Services, AVP Finance and Corporate Services	Approval Date	April 27, 2022

1.0 Purpose/ Background

NAIT processes credit card transactions through various channels and is therefore required to meet the requirements of Payment Card Industry and Data Security Standard (PCI-DSS) and other Card Brand Rules and Regulations. The potential penalties for non-compliance include lawsuits, insurance claims, loss of reputation and business, payment card issuer fines and government fines.

Effective handling of Cardholder Data requires the participation and support of every staff member who handles Cardholder Data, and it is the responsibility of the staff member to understand these procedures and conduct their activities accordingly.

2.0 Definitions

Term	Definition
Cardholder Data	At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder Data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code (the three or four-digit value in the magnetic stripe that follows the expiration date of the payment card on the track data).
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Payment Application	Any application that stores, processes, or transmits cardholder data electronically.

3.0 Procedures

3.1 General Procedures

3.1.1 The System Owner for each Payment Application must ensure appropriate staff is aware of this procedure and have completed NAIT's Security Awareness Program.

3.1.2 Prior to purchase or implementation of systems or services used to process credit card transactions the interested party will complete the NAIT PCI

Questions to Ask Vendors form to determine if the offering aligns with NAIT's current CDE (Cardholder Data Environment) strategy.

3.1.3 Implementation and changes to system components (including third party and outsourced solutions) that process, transmit or store cardholder data must be approved by the Associate Vice President, Finance and Corporate Services and the Chief Information Officer.

3.1.4 Payment Applications, even those certified as Payment Application Data Security Standard (PA-DSS) compliant, must be implemented in a PCI-DSS environment. Implementation or changes to all Payment Applications must be approved by the Associate Vice President, Finance and Corporate Services and the Chief Information Officer.

3.1.5 All system components that process, store or transmit card data, or those components connected to card data systems, including PIN entry devices, must reside on a network designated for PCI-DSS components.

3.1.6 All system components residing on NAIT's network designated for PCI-DSS must be approved devices and technologies.

3.2 Handling of Cardholder Data Procedures

3.2.1 Each department that processes credit card transactions must provide easy access to a cross-cut shredder. Crosscut shredding must take place immediately following the transaction for:

- cardholder Data written down for any reason
- cardholder Data received in hardcopy

3.2.2 Cardholder Data must be processed promptly. When the Cardholder Data cannot be processed immediately, the Cardholder Data must be stored in a secured location accessible by authorized personnel only.

3.2.3 The receipt of Cardholder Data in a card-not-present transaction is restricted to hardcopy format or via an ITS approved and installed analog phone.

3.2.4 Cardholder Data or Sensitive Authentication Data must never be recorded or forwarded in electronic format and must never be stored on local or network computing devices.

3.2.5 The inter-departmental transfer of hard copy media containing cardholder data must be approved prior to the transfer and accurately tracked.

3.2.6 PAN (primary account number) must be masked when displayed such that only personnel with a legitimate business reason can see more than the first six/last four digits of the PAN.

3.2.7 Suspicious behavior and indication of device tampering must be reported in accordance with IT 1.10 Security Incident Handling Procedure.

3.2.8 Cardholder Data handlers must complete NAIT's Security Awareness Program annually.

3.2.9 Remote access for vendors and business partners must be monitored while in use and deactivated when not in use.

3.2.10 Unacceptable handling of Cardholder Data

The following activities are prohibited. The list below is not exhaustive, but it provides a framework for appropriately handling of Cardholder Data:

3.2.10a Hard Copy Records

- Leaving Cardholder Data information unattended
- Throwing Cardholder Data information in the trash
- Copying or distributing Cardholder Data in any fashion
- Sharing Cardholder Data information with anyone who has no need to know the information

3.2.10b Electronic Records

- Entering Cardholder Data in any device or application that is not authorized
- Copying and storing Cardholder Data in any fashion
- Sharing Cardholder Data in any fashion with anyone who has no need to have access to the data

4.0 Exceptions to the Procedure

4.1 Exceptions to this procedure must be documented and formally approved by the Procedure Owner.

Procedure exceptions must include:

- the nature of the exception
- a reasonable explanation for why the procedure exception is required
- confirmation that the exception aligns with the general principles
- any risks created by the procedure exception and how they will be managed

5.0 Related Documentation

IT 1.4 Protection of card reading devices used in card present transactions
IT 1.3 Third-party IT Service Provider Management Policy
IT 3.1 Third-party IT Service Provider Management Procedure
IT 1.10 IT Security Incident Handling Procedure
NAIT PCI Questions to Ask Vendors

Document History

Date	*Action/ Change*
March 7, 2012	New Document (ITS ref DOC0010068 Rev 3.0)
May 18, 2018	Changed from Guideline to Procedure (ITS ref DOC0010068 Rev 4.0)
June 6, 2018	Clarify 4.1, 4.3 and 4.4 to meet PCI DSS requirements (ITS ref DOC0010068 Rev 5.0)
January 31, 2019	Addition of 2.2 and Addition of NAIT PCI Questions to Ask Vendor to 6.0 (ITS ref DOC0010068 Rev 0.6)
May 17, 2019	Remove second bullet under 4.10.2
December 21, 2020	Update titles and Add 1.4 to Related Documentation (ITS ref DOC0010068 Rev 0.8)
February 18, 2022	Update for title change; adopted new procedure template
January 19, 2023	Minor grammatical changes (ITS Ref DOC0010068 10.0)