3.17 Payment Card Industry (PCI) Compliance Policy

Policy Statement

The Government of Nova Scotia recognizes the importance of payment security related to the storage, processing and transmitting of client cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) has developed standards to mitigate the risk and ensure the proper handling of Payment Card transactions. To continue processing Payment Card transactions, the Government of Nova Scotia must adopt and comply with the PCI SSC standard, Payment Card Industry Data Security Standard (PCI DSS). This PCI Compliance Policy outlines the requirements which must be followed.

Definitions

CARD VERIFICATION CODE (CVC) OR CARD VERIFICATION VALUE (CVV)

A number that uniquely associates with each individual physical Payment Card with the credit card number. For VISA®, MasterCard® and Discover® branded credit cards, the CVV is a 3-digit number printed to the right of the signature panel area on the back of the card. For American Express® branded credit cards, it is a 4 digit code printed above the card number on the front of the card. The purpose of the CVV is to ensure that the cardholder has the credit card in hand when making a purchase for "card-not-present" transactions.

CARDHOLDER DATA (CHD)

Payment Card information including the primary account number by itself or with any of the following: cardholder name, expiration date and/or service code.

DEPUTY HEAD

The Deputy Minister or designate of a department, or the senior administrative officer of an agency not reporting through a Deputy Minister.

MERCHANT

Any government body (department, office, public service unit, etc.) that holds a merchant account under a Provincial Merchant Agreement, accepts payments and is subject to this policy.

PAYMENT CARD
Any client card that bears the logo of the founding members of the PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL (PCI SSC)
A security council founded by the five major credit card providers (American Express, Visa Inc., MasterCard Worldwide, Discover Financial Services and JCB International). The PCI SSC is the open global forum that maintains the Payment Card Industry standards.

PAYMENT PROCESSING VENDOR(S)
A vendor that provides Payment Card transaction processing and settlement to the Government of Nova Scotia Merchants.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)
A proprietary information security standard for organizations that process branded credit cards from the PCI SSC (including but not limited to Visa, MasterCard, American Express, Discover, and JCB).

PCI COMPLIANCE
Technical and operational requirements that businesses must follow to ensure that credit card data provided by cardholders is protected.

SELF-ASSESSMENT QUESTIONNAIRE (SAQ)
A fully annotated questionnaire completed by the Merchant, where responses to the PCI DSS SAQ need to be qualified (annotated) with supporting justifications.

TRANSACTION
For the purposes of this policy, a transaction is the processing of a Payment Card.

Policy Objectives

Adherence to the PCI DSS is required to process Payment Card transactions. This policy will promote compliance to the technical and operational requirements established within the PCI DSS. The policy objectives are to avoid penalties for non-compliance and reputational damage resulting from non-compliance. Penalties may include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.

Application

This policy applies to:

- Any individual that is involved in handling Payment Cards or Payment Card transactions for the purchase of Government of Nova Scotia products or services.
- Any individual that manages and/or supports staff involved in the acceptance of Payment Cards, and whose role gives the individual access to records, computer hardware and/or software that processes or retains the payment card information.
- Any individual that manages the Merchant account contract on behalf of the Province.
- Any individual in a position/role identified within the Accountability section.
- Any individual from Nova Scotia Digital Services (NSDS) Branch of Service Nova Scotia & Internal Services Department (SNSIS), or the Department of Finance & Treasury Board (FTB) that provides support to PCI Compliance – in particular banking and Merchant account contract management, and IT security and services.

This policy applies whether the processing is performed by the Government of Nova Scotia, or by an external third party acting as a service provider to the Government of Nova Scotia.

Policy Directives

The Government of Nova Scotia is fully committed to complying with the PCI DSS.

Compliance by the Government requires that:

1. Any Merchant setting up an operation to receive Payment Cards for the purchase of goods or services will require an approved merchant account.
2. Liability Management & Treasury Services (LMTS) Division within FTB is the only administrative area authorized to arrange for the creation of approved merchant accounts.
3. Client CHD cannot be sent/received by electronic messaging (i.e. email, instant messaging).
4. Client CHD must not be retained, unless there is an approved business case validated by both the Operational and IT Security Officers at FTB and SNSIS.
5. Cardholder information cannot be transmitted through the Provincial Data Network (PDN). This includes multifunction xerox machines, communication applications (email, Microsoft Teams, Skype, etc), network drives, other electronic

devices such as iPad and work cell phones, as well as recorded phone lines where phone transactions are permitted.

6. During the hiring process of transaction processing staff, appropriate background checks will include reference and credit checks, as identified in Corporate Administrative Policy Manual 500 (Human Resources Management), 2.5 Fair Hiring Policy.
7. Only authorized and trained individuals may accept and/or access Payment Card information. These individuals and their supervisors must ensure adequate training as described in the NS PCI Operational Procedures (OP).
8. Payment Cards may be accepted only using methods approved by the NS PCI Council.
9. Merchants wishing to accept Payment Cards via our web portal are to have merchant accounts set up via SNSIS.
10. Each person who has access to Payment Card information is responsible for maintaining the confidentiality of that information.
11. Payment Card information must be destroyed through acceptable means as per NS PCI OP 13 as soon as the transaction is complete. If required to be held longer, approval must be received by the Operational Security Officer and adherence to cardholder retention procedures must be followed.
12. Merchants must ensure that any systems implemented for the purpose of accepting Payment Cards must use the services of the NSDS branch of SNSIS, to ensure adequate IT standards have been incorporated.
13. Merchants must maintain appropriate controls over their processes by implementing the NS PCI OP.
14. Any software and hardware to be used by a Merchant to support its business operations related to Payment Card processing must be approved by NSDS branch of the SNSIS.
15. Merchants must have documented procedures for complying with this policy and the PCI DSS. These procedures must be in-line with NS PCI OP.
16. Suspected theft or compromise of Payment Card information must be reported immediately to PCISecurityTeam@novascotia.ca (See NS PCI OP 22A)
17. Merchant device inventory will be maintained by Merchants, PCI Liaisons and LMTS. This includes information required by the PCI DSS.

18. PCI Liaisons must notify LMTS when any changes in equipment take place to ensure the master inventory listing is accurately maintained.
19. PCI Liaisons must annually submit to the Operational and IT Security Officers a report, signed by their Deputy Head, regarding Merchant's compliance to PCI DSS, including:
    a. Security Awareness Training
    b. Site Assessment Results
    c. Compliance to NS PCI OP
    d. Compliance to this policy
20. Compliance gaps identified requiring remediation should be reported immediately to both the Operational Security Officer by the PCI Liaison.
21. The Operational Security Officer oversees the completion of PCI compliance reporting, as well as completing the Government of Nova Scotia SAQs.
22. The performance of IT testing requirements for PCI Compliance will be coordinated through the SNSIS, NSDS branch and reported to the IT Security Officer.
23. The Operational Security Officer will report PCI compliance to the NS PCI Council.

Policy Guidelines

Merchants should include PCI-related training into their staff orientation program for those operational areas that include Payment Card transaction processing.

Accountability

MERCHANT

Deputy Heads will:

- assign a PCI Liaison.
- assign a member to the PCI NS Council, if required.
- ensure Merchant is compliant with PCI DSS.
- submit annual report of compliance.

PCI Liaison will:

- be a member of the PCI Compliance Committee.
- manage the Merchant PCI compliance program.

FINANCE AND TREASURY BOARD

Operational Security Officer will:

- chair the PCI Compliance Committee.
- manage the corporate PCI Compliance Program.
- be a member of the PCI Compliance Management Team.
- be a member of the PCI NS Council, representing operations and as Secretary to the PCI NS Council.
- be a member of the PCI Security Team for Incident Management Response.

Manager Banking Agreements will:

- manage contracts and relationships with Merchant vendors.
- be a member and alternate chair of the PCI Compliance Committee.
- be a member of the PCI Compliance Management Team.
- be a member of the PCI NS Council, representing operations.
- be a member of the PCI Security Team for Incident Management Response.

SERVICE NOVA SCOTIA AND INTERNAL SERVICES

IT Security Officer will:

- manage the IT operations of the PCI Compliance Program.
- be a member of the PCI Compliance Committee.
- be a member of the PCI Compliance Management Team.
- be a member of the PCI NS Council, representing the IT operations.
- be a member of the PCI Security Team for Incident Management Response.

PCI COMPLIANCE COMMITTEE

Committee will:

- interpret and communicate PCI Compliance policy guidelines, and procedures for Merchants.
- submit recommendations to the PCI NS Council.

PCI NS COUNCIL

Council will:

- provide direction and guidance to those managing the PCI Compliance Program.

Monitoring

Department of Finance and Treasury Board is responsible for the review and update of this policy.

References

ACTS AND POLICIES

Freedom of Information and Protection of Privacy Act
PCI DSS Standards <www.pcisecuritystandards.org>
Manual 200, Chapter 9.1 Banking Services Policy
Manual 200, Chapter 11.5 Corporate Collection Policy
Manual 300, Chapter 4.1 Records Management Policy
Manual 300, Chapter 4.10 Information Management Policy
Manual 300, Chapter 4.11 Privacy Policy
Manual 500, Chapter 2.5 Fair Hiring Policy

Enquiries

PCI Management PCI Management@novascotia.ca

Approval date:	***December 16, 2015***	Effective date:	***December 16, 2015***
Approved by:	***Treasury and Policy Board***	Administrative update:	***September 23, 2021***