

3.17 Payment Card Industry (PCI) Compliance Policy

Policy Statement

The Payment Card Industry (PCI) Security Standards Council (SSC) has developed standards, referred to as the Payment Card Industry Data Security Standards (PCI DSS) to mitigate the risk and ensure the proper handling of Payment Card Transactions processed through automated systems and manual processes. The Nova Scotia Government, as a Merchant, must adopt and comply with the PCI SSC standards in order to continue processing Payment Card Transactions. 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 on. 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.

MERCHANT

Any organization or entity subject to this policy that accepts Payment Cards as payment for goods, services and/or donations, and has been authorized to do so by the Province of Nova Scotia.

MERCHANT ORGANIZATION

Any government body (department, office, public service unit, etc.) that is a merchant or holds a merchant account under the Provincial Merchant Agreements (See Appendix 3-D for listing).

PAYMENT CARDS

Any card that bears the logo of the founding members of 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 Province of Nova Scotia merchants.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

A proprietary information security standard for organizations that process branded credit cards from the PCI SSC (including Visa, MasterCard, American Express, Discover, and JCB).

PCI COMPLIANCE

Adherence to the PCI DSS that were developed to protect card information during and after a financial Transaction.

SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

A fully annotated questionnaire completed by the merchant, where responses to the PCI DSS Self-Assessment Questionnaire 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 Standards is required in order to process Payment Card Transactions. This Policy will promote compliance to the standards provided by PCI SSC. 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 all government departments and Merchant Organizations.

Within those organizations, this policy applies to:

- Any individual that is involved in handling Payment Cards or Payment Card Transactions for the purchase of Province 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 PCI organization structure identified in the Authority section.
- Any individual from Information, Communications and Technology (ICT) Services Branch of Internal Services Department (ISD), 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 Province of Nova Scotia, or by an external third party acting as a service provider to the Province of Nova Scotia.

Policy Directives

The Province of Nova Scotia is fully committed to complying completely with the Data Security Standards established by the Payment Card Industry. The organization structure in place for PCI Compliance is outlined in the Authority section.

Compliance by the Province requires that:

1. Any Merchant Organization 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. CHD cannot be transmitted/received by electronic messaging (i.e. email, instant messaging).

4. CHD must not be retained, unless there is a business case that shows the requirement of these records. Where a business requirement exists, CHD is deemed personal information, and as such needs to be well secured with access to it restricted to only those staff/management that require it for business purposes. These situations and set ups will be approved by both the Operational and IT Security Officers at FTB and ISD.
5. During the hiring process of transaction processing staff, appropriate background checks will include both reference and credit checks, as identified in MM500 Chapter 2.5 Fair Hiring Policy.
6. All users and supervisors must ensure adequate training as described in the NS PCI Operational Procedures are completed. Only authorized and trained individuals may accept and/or access Payment Card information.
7. Payment Cards may be accepted only using methods approved by the NS PCI Council.
8. Province of Nova Scotia departments that wish to accept Payment Cards via web portal are to have merchant account set up via Service Nova Scotia (SNS).
9. Each person who has access to Payment Card information is responsible for maintaining the confidentiality of that information.
10. Payment Card information must be destroyed through acceptable means as soon as it is no longer necessary or required.
11. Departments must ensure that any systems implemented for the purpose of accepting Payment Cards must use the services of the ICT Services Branch of ISD, to ensure adequate IT standards have been incorporated.
12. Departments must maintain appropriate controls over their processes by implementing the NS PCI Operational Procedures.
13. Any software and hardware to be used by a Merchant to support its business operations related to Payment Card processing must be approved by ICT Services branch of the ISD.
14. Each department that handles payment card information must have documented procedures for complying with this policy and PCI- DSS. These procedures must be in-line with Procedures identified in the Related Documents.
15. Suspected theft or compromise of payment card information must be reported immediately to the Security Officers at both FTB and ISD, as well as to Information, Access and Privacy (IAP) Services as a privacy breach.

16. Master Merchant device inventory will be maintained by Finance & Treasury Board, LMTS which will include information required by the PCI Standards.
17. Departmental PCI Liaisons must notify LMTS when any changes in equipment take place to ensure the master inventory listing is accurately maintained.
18. Departmental PCI Liaisons must annually submit to both the Operational and IT Security Officers a report (see report template in Related Documents section), signed by their Deputy Minister, regarding their department's compliance to the PCI DSS, including:
 - a. Security Awareness Training
 - b. Site Assessment Results
 - c. Compliance to standard procedures
 - d. Compliance to this policy
19. The deadline for submitting the Departmental PCI Compliance report will be established and communicated by the NS PCI Council to the Deputy Ministers.
20. Any compliance gaps identified during the departmental assessments requiring remediation should be reported as soon as possible to both the Operational and IT Security Officers by the Departmental PCI Liaisons.
21. Security Officers oversee the completion of departmental compliance reporting, as well as performing the Provincial SAQ.
22. The performance of IT testing requirements for PCI Compliance will be coordinated through the ISD, ICT Services Branch, and reported up to the IT Security Officer.
23. Both Operational and IT Security Officers will report the corporate compliance up to the NS PCI Council.
24. Merchant Organizations must make every reasonable effort to comply with the physical security requirements identified in the PCI DSS standards.

Failure to comply with these principles, as implemented in this policy, may result in the revocation of the ability to process credit card Transactions and/or lead to disciplinary action.

Policy Guidelines

- Departments should include PCI-related training into their staff orientation program for those operation areas that include payment transaction processing.

Accountability

The table shows the policy responsibilities based on the various roles created from the organization structure identified in the Authority Section.

Role	Applicable Organization(s)	Policy Accountability
Deputy Heads	<ul style="list-style-type: none"> · Merchant Organizations 	<ul style="list-style-type: none"> · Assigning a PCI Liaison to the PCI Compliance Committee · Ensuring Departmental compliance to this policy · Reporting on the compliance using the applicable reporting template
NS PCI Council	<ul style="list-style-type: none"> · Finance & Treasury Board · ISD (ICT Services) · 3 largest Merchant Organizations 	Overall Direction and Guidance
Manager Banking Agreements	<ul style="list-style-type: none"> · Finance & Treasury Board 	<ul style="list-style-type: none"> · Chair – PCI Compliance Committee · Liaison between departments and merchant account vendor · Master – Merchant Account Inventory
IT Security Officer	<ul style="list-style-type: none"> · ISD (ICT Services) 	<ul style="list-style-type: none"> · Development of IT Security Standards · Ensure IT Compliance Requirements are Complete · Report on compliance for these
Operational Security Officer	<ul style="list-style-type: none"> · Finance & Treasury Board 	<ul style="list-style-type: none"> · Develop Operational Standard Procedures · Coordinate the annual compliance attestation based on the PCI Merchant Level
Departmental PCI Compliance Liaison	<ul style="list-style-type: none"> · All Merchant Organizations 	<ul style="list-style-type: none"> · Manage PCI Compliance within the department to ensure all aspects of this policy are adhered to, documented, and reported to the Security Officers
PCI Compliance Committee	<ul style="list-style-type: none"> · Manager Banking Agreements · IT Security Officer · Operational Security Officer · Departmental PCI Compliance Liaisons 	<ul style="list-style-type: none"> · Manage PCI Compliance for the government to ensure all aspects of this policy are adhered to, documented, and reported through the SAQ.

Monitoring

NS PCI Council along with the PCI Security Officers at FTB, and ISD, and the Manager of Banking Agreements will monitor the policy for implementation, performance, and effectiveness.

References

ACTS AND POLICIES:

Freedom of Information and Protection of Privacy Act

PCI DSS Standards [www.pcisecuritystandards.org]

MM200 Chapter 9.1 Banking Services Policy

MM200 Chapter 11.5 Corporate Collection Policy

MM300 Chapter 4.1 Records Management Policy

MM300 Chapter 4.10 Information Management Policy

MM300 Chapter 4.11 Privacy Policy

MM500 Chapter 2.5 Fair Hiring Policy

RELATED DOCUMENTS

- Operational Standard Procedures
- Mobile Device Procedures
- IT Security Standards
- Pin Pad Procedure
- PCI Compliance Report – Merchant Organization
- PCI Compliance Report – IT Security Officer
- PCI Compliance Report – Operational Security Officer

Enquiries

Manager Cash Management Services, FTB	902 424-3841
Operational Security Officer, FTB	902 424-3456
IT Security Officer, ISD (via Service Desk)	902 424-7777

Authority

PCI Compliance will be jointly the responsibility of the FTB and the ISD. The authority for the development and oversight of the Payment Card Acceptance Policy is the responsibility of the NS PCI Council which includes the following positions:

- Chief Information Officer
- Controller
- Senior Management representation from the three largest merchant organizations.

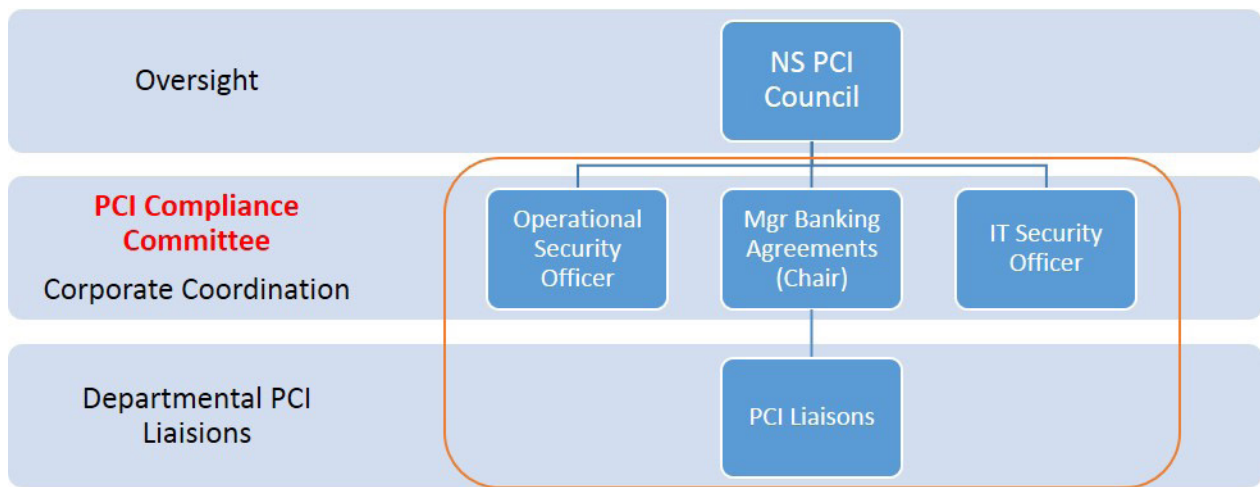
The NS PCI Council’s role is to ensure the continued acceptance of Payment Cards in government and provide overall direction and guidance to Merchants to ensure the Province achieves and maintains compliance with the PCI DSS.

Reporting up to the NS PCI Council will be the 2 Security Officers (one IT from ISD, ICT Services Branch; and one Operational from FTB), and the Manager of Banking Agreements (with Liability Management & Treasury Services Division at FTB).

Each Department that accepts Payment Cards will be required to identify a Departmental PCI Liaison. This person will manage the PCI Compliance aspects within that department. All the Departmental PCI Liaisons, IT Security Officer and Operational Security Officer will form the PCI Compliance Committee, chaired by the Manager of Banking Agreements. PCI Compliance Committee is responsible for:

- o Interpretation and communication of PCI Compliance policy, guidelines and procedures for the province;
- o Approval of Payment Processing Vendors, scanning vendors and also qualified security assessors;
- o Approval of Merchants;
- o Providing the departmental documentation required to report compliance based on the methods required by PCI based on our Merchant Level;
- o Review and acceptance of the Merchant’s fully annotated response to the compliance reporting required by PCI; and
- o Responsible for the revocation of a Merchant’s capabilities.

Responsibility for all the on-line payment approaches resides with Information, Communications & Technology Services branch of ISD.



Approval date: **December 16, 2015**
 Approved by: **Treasury and Policy Board**

Effective date:
 Administrative update: **April 26, 2019**

Appendix 3-D

Merchant Organizations included in the Provincial Merchant Agreement:

- Department of Internal Services – Accounts Receivable
- Office of Service Nova Scotia
- NS Apprenticeship Agency
- Department of Education & Early Childhood Development
- Department of Lands and Forestry
- Department of Justice
- Department of Communities, Culture & Heritage
- Department of Health and Wellness
- Department of Agriculture
- Department of Transportation & Infrastructure Renewal
- Metropolitan Regional Housing Authority
- Cape Breton Island Housing Authority
- Cobequid Housing Authority
- Eastern Mainland Housing Authority
- Western Housing Authority