AD16  Payment Card Industry Data Security Standards

Classification: Administration
Responsible Authority: Chief Digital Officer, Information Technology Services
Executive Sponsor: Vice President, Finance and Administration
Approval Authority: Algonquin College Executive Team
Date First Approved: 2013-07-02
Date Last Reviewed: 2019-11-01
Mandatory Review Date: 2020-11-02

PURPOSE
This policy sets forth the guidelines required by the College regarding Payment Card Industry Data Security Standards (PCI DSS) for processes and technology involved in acceptance, processing, and transmission of debit and credit cardholder account data.

SCOPE
This policy applies to all Algonquin College business units, departments, and their employees (which includes faculty, staff and students) involved in accepting, processing, or transmitting cardholder account data for payments on behalf of Algonquin College. This includes all payment transactions involving credit cards, debit cards, or pre-paid cards branded with one of the five payment card brands that are part of the PCI Security Standards Council (Visa, MasterCard, American Express, JCB International and Discover Financial).

DEFINITIONS
Payment Card Industry Data Security Standards (PCI DSS) Definitions

<table>
<thead>
<tr>
<th>Word/Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquirer</td>
<td>Also referred to as “merchant bank,” “acquiring bank” or “acquiring financial institution.” An entity that initiates and maintains relationships with merchants for the acceptance of payment cards.</td>
</tr>
<tr>
<td>Cardholder Data</td>
<td>At a minimum, cardholder data consists of the full payment card Primary Account Number (PAN). Cardholder data may also exist in the form of the full PAN, plus any of the following: cardholder name, expiration date and/or service code.</td>
</tr>
<tr>
<td>Card Verification Code or Value</td>
<td>The rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the primary account number (PAN) on the face of all payment cards.</td>
</tr>
<tr>
<td>Cardholder Account Data</td>
<td>Consists of cardholder data and sensitive authentication data.</td>
</tr>
<tr>
<td><strong>Cardholder Data Environment (CDE)</strong></td>
<td>The people, processes and technology involved in acceptance, processing or transmission of cardholder account data, including any connected system components.</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>PCI DSS</strong></td>
<td>Acronym for “Payment Card Industry Data Security Standard”. PCI DSS was developed to enhance cardholder data security and facilitate consistent data security measures by providing a baseline of technical and operational requirements designed to protect cardholder data.</td>
</tr>
<tr>
<td><strong>PA-DSS</strong></td>
<td>Acronym for “Payment Application Data Security Standard”. It covers secure payment applications to support PCI DSS compliance.</td>
</tr>
<tr>
<td><strong>PCI SSC</strong></td>
<td>Acronym for “PCI Security Standards Council”. PCI SSC is an independent body providing oversight of the development and management of PCI DSS. The founding members of PCI SSC are Visa, MasterCard, American Express, JCB International, and Discover Financial.</td>
</tr>
<tr>
<td><strong>Payment Brands</strong></td>
<td>The founding members of PCI SSC, which are Visa, MasterCard, American Express, JCB International, and Discover Financial.</td>
</tr>
<tr>
<td><strong>Payment Card</strong></td>
<td>Credit card, debit card or pre-paid card branded with the logo of any of the payment brands.</td>
</tr>
<tr>
<td><strong>Merchant</strong></td>
<td>An entity that accepts payment cards bearing the logos of any of the five members of the PCI SSC as payment for goods and/or services.</td>
</tr>
<tr>
<td><strong>Merchant Account</strong></td>
<td>A bank account that enables the holder to accept payment cards bearing the logos of any of the five members of the PCI SSC.</td>
</tr>
<tr>
<td><strong>Network Segmentation</strong></td>
<td>Also referred to as “segmentation” or “isolation”, network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the Cardholder Data Environment and thus reduces the scope of the PCI DSS assessment.</td>
</tr>
<tr>
<td><strong>Payment Card Privilege</strong></td>
<td>Refers to the privilege which merchants have to accept payment cards for payment transactions.</td>
</tr>
<tr>
<td><strong>SAD</strong></td>
<td>Acronym for “Sensitive Authentication Data”. It represents security-related information (including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.</td>
</tr>
<tr>
<td><strong>SAQ</strong></td>
<td>Acronym for “Self-Assessment Questionnaire”. It is an assessment document that is used by a merchant to validate its own compliance with the PCI DSS. Algonquin College utilizes several different SAQs covering its various merchant account areas.</td>
</tr>
<tr>
<td><strong>System Component</strong></td>
<td>Any network component, server, or application included in or connected to the Cardholder Data Environment.</td>
</tr>
</tbody>
</table>
### Algonquin College Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algonquin College Merchant</td>
<td>A business unit, department, and their employees (which includes faculty, staff, and students) authorized by Algonquin College to process payment card transactions on behalf of the College.</td>
</tr>
<tr>
<td>Merchant Account Owner</td>
<td>The manager responsible for an Algonquin College business process that involves the acceptance of payment cards into a Merchant Account.</td>
</tr>
</tbody>
</table>

### POLICY

1. **PCI DSS Compliance Requirements:**
   As a merchant that collects, processes and transmits cardholder data, Algonquin College is required to be PCI DSS compliant by the PCI Security Standards Council (PCI SSC). Non-compliance exposes the College to significant risks including but not limited to:
   - Payment card compromise, theft and financial fraud;
   - Cardholder identity theft;
   - Incident response and security breach recovery costs;
   - Fines and penalties for compromise, including increased cost per processed transaction;
   - Termination of payment card privileges;
   - Prevention from entering into new lines of business;
   - Loss of customer trust and business;
   - Damage to reputation and brand; and
   - Legal liabilities.

2. **Algonquin College Merchant Accounts:**
   Any department or business unit setting up an operation to process payment card transactions must formally request and receive an approved Algonquin College merchant account prior to processing any payments.

   Algonquin College Treasury Department is the only administrative body authorized to create/open merchant accounts. All merchant accounts must be approved in writing by Treasury Department. All merchant accounts must have an associated Merchant Account Owner.

3. **Opening Bank Accounts:**
   All Algonquin College departments and/or business units are prohibited from opening a bank account or any type of account (e.g. PayPal) to receive payments in the name of the College.

   Algonquin College Treasury Department is the only business unit authorized to establish bank accounts to receive payments on behalf of the College. This includes all bank accounts bearing a College campus address.

4. **Director, Finance and Administrative Services:**
Provides management oversight for all Finance related decisions and directions with respect to payment cards and reconciliations.

5. Treasury Supervisor, Finance:
Provides day-to-day management of Algonquin College merchant accounts, including the review and approval of requests for new accounts or changes to existing accounts, and liaising with the College’s acquirer.

6. Chief Digital Officer (CDO), Information Technology Services (ITS):
Provides management oversight for all IT related decisions and directions with respect to the card data environment.

7. Senior Manager, Information Security and Data Privacy (ITS):
Provides oversight and governance for all Algonquin College PCI DSS compliance related matters, including the authority to review and audit all payment related systems. All initiatives and projects to be carried out on behalf of Algonquin College which involve payment card processing must be reviewed and approved by the Senior Manager prior to implementation, and must comply with requirements specified by the College and the PCI DSS compliance standards. The Senior Manager is responsible for formal PCI DSS communications within the College, including the maintenance of a PCI DSS stakeholder advisory committee. The Senior Manager may delegate his/her responsibilities as appropriate.

8. Merchant Account Owners:
Algonquin College Merchant Account Owners are staff responsible for an Algonquin College business process that involves the acceptance of payment cards. They are responsible for ensuring the people, processes and technologies involved in accepting, processing or transmitting cardholder data within their area, including connected or supporting systems, comply with the PCI DSS and related Algonquin College policies, standards and procedures.

9. Electronic Storage and Transmission of Cardholder Account Data:
Cardholder account data must not be stored electronically anywhere within the Algonquin College IT environment (e.g. computer systems, network drive, database server) nor transmitted/received by electronic messaging (e.g. email, instant messaging).

Email is not an acceptable method of sending or receiving credit card account information. Emails received containing card holder data must be deleted immediately.

10. Paper Retention and Disposal:
Paper records of financial transactions that contain cardholder data must be securely stored at all times. Records are to be retained for a limited period consistent with the needs of the business. Storage and retention period must be approved by the Senior Manager, Information Security and Data Privacy.

11. External Parties Contractual Agreements:
Due diligence must be followed when engaging external parties to provide solutions and services related to the College’s PCI DSS program.
All external parties including but not limited to solution providers, service providers, program assessors, and acquirers, must be contracted using a written agreement that details their involvement, activities and responsibilities related to the College’s PCI DSS program. This agreement, which must be approved by the Senior Manager, Information Security and Data Privacy, must detail the protection mechanisms afforded to any cardholder data held in their possession.

12. Incident Response:
In the event of a security incident related to Algonquin College payment processes or systems in-scope for PCI DSS compliance, such as a security breach of cardholder data, the Senior Manager of Information Security and Data Privacy must be notified immediately, and is responsible for leading the execution of the PCI DSS Security Incident Response Plan.

13. Change Management:
Any change to Algonquin College business processes, systems, infrastructure or applications that have or might have a PCI DSS compliance implication, or that impacts processing of credit card payments, must be reviewed and approved by the Senior Manager, Information Security and Data Privacy prior to implementation.

Any minor or major changes, or maintenance activities to Algonquin College systems, infrastructure or applications that may impact the PCI DSS environment, PCI DSS compliance or the processing of debit and credit card payments must be formally documented in a change log. All changes must be detailed as well as adequately maintained and archived. This applies to changes made by employees, vendors, and third-parties.

14. Accounts and Privileges:
User accounts with access to systems in scope for PCI DSS compliance must be restricted to least privileges necessary to perform job responsibilities. Privileged accounts for individuals must be assigned based on job function, and must be authorized by the Merchant Account Owner or delegate.

Accounts and privileges assigned to individuals who are no longer employees, or who no longer have payment process related responsibilities, must be terminated immediately.

15. System Configuration and Operations:
For all systems in-scope for PCI DSS compliance, Algonquin College system configuration standards and operational security procedures must be followed for configuring and operating network and firewall components, application components, servers and all other system components.

16. Technology Use:
No technology systems shall be used within the security controlled Cardholder Data Environment, nor shall any user access to technology systems be authorized unless:
- Explicit approval by the Senior Manager, Information Security and Data Privacy is obtained, prior to implementation.
- A list of all such technology systems is provided to the Senior Manager, Information Security and Data Privacy, and the list maintained thereafter.
• Specific acceptable network locations for and usage of technology systems is defined and approved.
• All technology systems are appropriately labeled with information that references system owner, contact information and purpose.
• Strong, multi-factor authentication is used for remote access to the Cardholder Data Environment. Remote Access is any access that originates from outside the Algonquin network, such as employees working from home or vendors providing support from remote locations.
• Remote access technologies used by external party vendors and solution providers are only activated for specific periods when needed, and automatically disconnect after that time as well as when there is a specific period of inactivity.
• Payment applications are PA-DSS approved and validated as per the following: https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications

17. **Awareness Program:**
Employees with work functions that include accepting, transmitting and/or processing payment card information must, upon being hired, read the Algonquin College PCI DSS policy and undergo an initial mandatory security awareness and training program. These employees must subsequently participate within a mandatory PCI DSS Employee Awareness Training Program on an annual basis. Each Merchant Account Owner is responsible for ensuring that their required team members complete the training.

18. **Policy Review:**
The Algonquin PCI DSS policy and procedures must be reviewed at least annually and updated as required to reflect changes to PCI DSS standards, other regulations, policies, business objectives or changes to the Cardholder Data Environment.

19. **Policy Compliance:**
All Algonquin College people, process and technology that support business processes involving payment cards must comply with this policy. Failure by Algonquin College Merchant Account Owners to comply with this policy to the satisfaction of the Senior Manager, Information Security and Data Privacy may result in the revocation of the Merchant Account Owner’s payment card privileges.

## PROCEDURE

<table>
<thead>
<tr>
<th>ACTION</th>
<th>RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PCI DSS Compliance Oversight and Governance</td>
<td>Senior Manager, Information Security and Data Privacy, Merchant Account Owners</td>
</tr>
<tr>
<td>1.1 Achieve and maintain Algonquin College PCI DSS annual compliance certification.</td>
<td></td>
</tr>
</tbody>
</table>
1.2 Utilize and document appropriate PCI DSS Self-Assessment Questionnaire(s) (SAQs) annually on behalf of the entire College.

1.3 Review annual PCI DSS SAQs and provide attestation to their accuracy and completeness.

1.4 Provide appropriate interpretation and communication of PCI DSS compliance guidelines and best practices.

1.5 Ensure that Algonquin College contractual agreements, where applicable, stipulate adherence to PCI DSS requirements.

1.6 Implement a formal PCI DSS Awareness Training program to educate employees on the importance of PCI DSS compliance.

2. Management of Algonquin College Merchant Accounts

2.1 Make requests for new merchant account number and/or Point of Sale (POS) devices in writing to Treasury Department

2.2 Provide business case (if required) for new merchant number or Point of Sale device.

2.3 Provide sufficient details of intended business processes to the Senior Manager, Information Security and Data Privacy to determine the relevant sections of the appropriate PCI DSS SAQ to be completed.

2.4 Review and approve submitted business cases for all prospective Merchant Account Owners.

2.5 Provide written approval and instruction to the new Algonquin College Merchant Account Owner.

2.6 Implement an appropriate payment solution for an approved Algonquin College merchant after approval by Treasury Department

2.7 Respond to relevant sections of the appropriate PCI DSS SAQ and submit information and evidence to the Senior Manager, Information Security and Data Privacy for review.

2.8 Review and validate Algonquin College Merchant Account Owner responses to the appropriate PCI DSS SAQ.

2.9 Revoke Algonquin College merchant payment card privileges as deemed appropriate.
3. Implementation, Controls, and Processes

3.1 Develop and maintain business process controls in compliance with PCI DSS requirements and as advised by the Senior Manager, Information Security and Data Privacy.

3.2 Design, integrate and implement payment solutions for all Algonquin College Merchant Account Owners in compliance with PCI DSS requirements, including the development or the purchase of appropriate software or services to be used by Algonquin College Merchant Account Owners.

3.3 Maintain, support and monitor Algonquin College system components in compliance with PCI DSS requirements.

3.4 Restrict access to records on a business need-to-know basis. Securely store paper records of cardholder data only for a specific limited retention period and only if there is a business justification. At the end of the retention period, ensure that records are crosscut shredded, incinerated or otherwise securely destroyed to ensure that records cannot be reconstructed.

3.5 Maintain an up-to-date list of devices that capture payment card data via direct physical interaction. The list must include - at a minimum - the make, model, serial number, owner and location of each device.

SUPPORTING DOCUMENTATION
PCI DSS Compliance - Payment Terminal Security Procedures

RELATED POLICIES
IT01 - Acceptable Use of Computer Networks and Accounts
IT05 - Information Sensitivity and Security

RELATED MATERIALS
PCI DSS Standards and Supporting Documents
https://www.pcisecuritystandards.org/document_library