PAYMENT CARD POLICY

PURPOSE

The University is committed to safeguarding personal and account information, including when accepting debit or credit cards ("payment cards") for payments.

The acceptance by the University of payment cards, specifically credit cards, is conditional on compliance with the Payment Card Industry's Data Security Standards ("PCI DSS"). The Payment Card Industry Security Standards Council has established stringent security requirements to safeguard credit card data through the PCI DSS. Compliance with the PCI DSS is a contractual requirement, and applies to all entities that store, process or transmit cardholder data.

This means that all University departments / areas ("merchants") that accept credit cards must be PCI DSS compliant. In addition, any affiliated or unaffiliated party involved with accepting / processing / transmitting credit card payments or storing credit card data on behalf of University merchants must be PCI DSS compliant, and furthermore, must provide ongoing valid proof of compliance to the University. The University is contractually obligated to identify such parties' responsibilities for securing cardholder data and monitor such parties' PCI DSS compliance.

Accordingly, this Policy establishes the security requirements for individuals and technologies involved in the processing / transmission of payment card data in order to safeguard against the disclosure and possible theft of cardholder data, and to comply with the PCI DSS requirements. Key responsibilities related to the achievement and maintenance of compliance with the PCI DSS are also outlined.

SCOPE

This Policy applies to University merchants and to the people, processes and technologies that process / transmit cardholder data. This includes the people, processes and technologies both

at, or on behalf of, the University, and also includes both electronic and paper documents associated with payment cards.

POLICY STATEMENT

People

Access to cardholder data must be limited to only those individuals whose job responsibilities require this access. Access must be limited to the least amount of information required in order to allow the individuals to perform their job responsibilities.

Individuals with access to cardholder data must not share cardholder information with anyone else without documented approval by their supervisor.

Individuals are prohibited from copying or moving stored cardholder data unless explicitly authorized for a defined purpose by their supervisor.

Processes

The Primary Account Number (PAN) must be masked when displayed (the first six and last four digits are the maximum number of digits permitted to be displayed). This applies not only to paper receipts but also to systems / solutions in use for payment card related purposes.

Prior approval by Financial Services is required for areas / departments to obtain a merchant identification number from the University's acquirer.

Transactions related to cardholder data received via email / voicemail / social media must not be processed.

No electronic storage of cardholder data is permitted on premise. No electronic storage of cardholder data is permitted in the cloud without industry-standard PCI-compliant tokenisation.

Cardholder data may be stored on paper provided such documents are physically secured. The retention period for such documents must be limited to that which is required for a University, legal and/or regulatory purpose. When no longer

required, such documents must be cross-cut shredded and disposed of in a secure manner.

The card validation code or value (three- or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions must not be stored under any circumstances.

A cardholder's personal identification number (PIN) must not be stored under any circumstances.

A current inventory of PIN transaction security (PTS) devices must be maintained. PTS devices must be inspected periodically and a log of inspections must be maintained by University merchants.

Technologies

Prior approval of the IT Steering Committee or designate is required for any area / department wishing to accept payment cards in any manner and / or to implement any payment systems / solutions, whether on premise, in the cloud, hosted or software as a service.

Remote access technologies and / or access methods utilized by vendors / service providers to access cardholder data or the cardholder data environment must only be activated when explicitly needed and must be deactivated immediately after use.

Service providers

Where a service provider stores, processes or transmits cardholder data on behalf of a University merchant:

- The merchant's process for engaging the service provider must include verifiable proper due diligence prior to engagement. Only PCI DSS compliant service providers must be engaged;
- The merchant must monitor the service provider's PCI DSS compliance status (e.g., by requesting and reviewing

the annual "Self-Assessment Questionnaire and Attestation of Compliance for Service Providers");

- The written agreement with the service provider must include the service provider's acknowledgement that the service provider is responsible for the security of cardholder data that it stores / processes / transmits on behalf of the University merchant;

- The merchant must create and maintain a complete list of service providers that can access any University point-of-sale system or cardholder data.

Anyone who learns of an actual or potential cardholder data security breach must immediately inform the Associate Vice-President, Information Technology Services and / or the Associate Vice-President, Financial Services.

DEFINITIONS

The official "Glossary of Terms, Abbreviations, and Acronyms" as defined by the PCI Security Standards Council can be found here (download available): https://www.pcisecuritystandards.org/document_library

COMPLIANCE AND REPORTING

The Associate Vice-President, Information Technology Services or the Associate Vice-President, Financial Services may terminate payment card privileges for any merchant not in compliance with this Policy.

The Associate Vice-President, Information Technology Services and the Associate Vice-President, Financial Services will update SAC on policy violations as required.

Policy Owner:	Vice-President, Administration
Policy Lead:	Associate Vice-President, Information Technology Services Associate Vice-President, Financial Services
Policy Classification:	Operational
Approval:	Approved by the Executive Team
Effective date:	April 2021
Next review:	March 2023
Revision history:	Adopted 2017 Revised March 2018 Revised April 2021
Related documents:	Payment Card Standards Cloud / Hosted / SaaS Policy