Customer Credit Card Policy

Intent

Alma Mater Society of Queen's University is committed to providing our customers with consistently high levels of customer service. In the pursuit of our commitment, Alma Mater Society of Queen's University will strive to ensure that the proper security channels are in place to protect customer information gathered through credit card transactions.

In compliance with the Payment Card Industry's (PCI) Security Standards Council, the following guidelines shall be maintained by Alma Mater Society of Queen's University in order to ensure all credit card security standards are met.

Scope

This policy applies to all AMS waged and salaried employee positions, held by students of Queen's University.

Guidelines

Alma Mater Society of Queen's University shall ensure that the following PCI requirements are implemented and maintained at all times: (information sourced from PCI Data Security Standard: Understanding the Intent of the Requirements)

Alma Mater Society of Queen's University shall build and maintain a secure network by:

- Installing and maintaining a firewall configuration to protect cardholder data;
- Not using vendor-supplied defaults for system passwords and other security parameters. Passwords will be changed and internal security parameters shall be enhanced;
- Establishing a firewall which is maintained by the internal AMS IT department; and
- Utilize POS systems to complete all transactions, where there is a POS system in place.

Alma Mater Society of Queen's University shall protect cardholder data by:

- Implementing measures to protect any stored cardholder data;
- Ensuring encrypting transmission of cardholder data across open, public networks; and
- Use Moneris and/or POS systems to ensure no cardholder data is stored and that all information is encrypted.

Alma Mater Society of Queen's University, in conjunction with Queen's IT Department, where appropriate, shall maintain a vulnerability management program by:

- Using and regularly updating anti-virus software; and
- Developing and maintaining secure systems and applications.

Alma Mater Society of Queen's University will implement strong access control measures by:

- Restricting access to cardholder data by business need-to-know;
- Assigning a unique ID to each person with computer access; and

Alma Mater Society of Queen's University will regularly monitor and test networks including:

- Tracking and monitoring all access to network resources and cardholder data; and
- Regularly testing security systems and processes

Alma Mater Society of Queen's University shall implement an information security policy, which will be regularly reviewed and updated through POS upgrades, to:

- Address and maintain information security

Retention

Alma Mater Society of Queen's University shall keep to a minimum the credit card information that is retained through transactions. The Company shall only collect and retain required information for business purposes.

Alma Mater Society of Queen's University shall keep records under lock and key and ensure that access is available only to staff with a need to know. Credit card slips and related information shall always be stored in a locked till, and filed in a locked file cabinet/room. All credit card information is processed via Moneris or an online platform (such as Shopify). Any slips produced by these systems will only show the last 4 digits of the card, all other information is blocked.

Alma Mater Society of Queen's University shall only keep records containing personal information for the length of time in which there may be a need for keeping them. The maximum time personal information records collected from credit card use shall be stored is for one year.

Alma Mater Society of Queen's University shall ensure the proper destruction of all personal information. Paper records containing personal information must be shredded and disposed of. Any electronic records containing personal information must permanently be deleted by secure measures or render the personal information non-identifying so that it can no longer be used to identify an individual.

General Responsibilities for Alma Mater Society of Queen's University Employees

Employees shall:

- Store all physical documents containing credit card data in a locked drawer, locked file cabinet, or locked office;
- Maintain strict control over the internal and external distribution that contains credit card data;
- Change vendor supplied or default passwords;
- Ensure passwords conform with Computing Services rules and recommendations;
- Properly dispose of any media containing credit card data; and

- Upon receiving an unencrypted email from a customer with credit card data, employees shall notify the customer that they should no longer send this information via email and delete email immediately.

Employees must not:

- Transmit cardholder's credit card data by e-mail or fax;
- Store credit card data for repeat customers on paper in an unsecured area;
- Store Personal Identification Numbers (PINs);
- Electronically store on the Company's computer file or server any unencrypted credit card data;
- Electronically store any credit card data on any laptop or PC;
- Share user IDs for systems access; and
- Acquire or disclose any cardholder's data without the cardholder's consent.

Each credit card brand has its own program for compliance, validation levels, security and enforcement. More information about brand-specific security measures can be found on the credit card companies' websites.

Monitoring

Responsibility and/or contact person	Information Technology Office and Operations Office
Approved by	Board of Directors
Date initially approved	October 27, 2022
Date last revised	October 27, 2022
Date of next review	Every two years, or when significant change dictates a need for revision.
Related policies, procedures, and guidelines	Payment Card Industry's (PCI) Security Standards
Policies superseded by this policy	N/A