CREDIT CARD SECURITY POLICY

Effective Date: May 1, 2014

Originating Office: Office of the Chief Financial Officer

Supersedes /Amends: N/A

Policy Number: CFO-9

PREAMBLE

This Policy explains the credit card security requirements as provided for by the Payment Card Industry ("PCI") Data Security Standard Program. Concordia University (the "University") wishes to ensure the protection of information utilized by the University in attaining its business goals.

PURPOSE

The purpose of this Policy is to have PCI requirements apply to all University's systems that store, process, or transmit credit card holder data. The University's use of credit cards is limited to payment applications that are connected to the internet, and should normally not include storage of credit card holder data on any computer system.

This Policy does not supersede any provisions of any other relevant University Policy and should be read in conjunction with the *Code of Rights and Responsibilities* (BD-3), *Policy Concerning the Protection of Personal Information* (SG-9) and *Policy on Computing Facilities* (VPSS-30).

SCOPE

This Policy applies to all authorized permanent faculty, staff or external contractors of the University whose functions grant them access to credit card systems or credit card holder data, on any media ("Authorized Users") as well as any entities or individuals who intend to use credit card transactions on behalf of the University.

POLICY

1. The Chief Financial Officer of the University shall be responsible for the application of this Policy.

2. The Chief Financial Officer of the University shall be responsible for ensuring that this Policy and any associated guidelines, procedures and standards are reviewed at least annually and amendments shall be recommended as needed.

3. No member of the University shall install credit card systems without prior authorization from Financial Services.

4. It is the responsibility of Financial Services to secure credit card systems and credit card holder data, in any media, by:

   - Authorizing the installation and assisting in installing the required equipment for credit card transactions and maintaining an up-to-date inventory of such equipment per the University's *Policy on Capital Asset Management* (CFO-4);

   - limiting access to the University's credit card systems and to credit card holder data to Authorized Users only, in collaboration with the relevant units, and maintaining a centralized list of such Authorized Users;

   - taking measures and issuing Guidelines to Authorized Users, as needed, to ensure the safekeeping and destruction of credit card holder data when such data is no longer needed;

   - ensuring that measures are taken to qualify only PCI certified external contractors as Authorized Users and ensuring that proper legal documents are executed to the satisfaction of the University prior to granting Authorized Users access to any credit card systems or credit card holder data;

   - pursuant to consultation with the relevant units, removing the status of Authorized Users from individuals whose functions no longer require access to credit card systems or credit card holder data;

- informing Authorized Users of their responsibility for detecting security incidents in order to facilitate the incident response plan and procedures;
- reporting all information regarding technological security incidents ("IT Incident") to the applicable credit card associations, credit card service providers and, where necessary, to the local authorities, in collaboration with the relevant units.

5. It is the responsibility of the University's Instructional & Information Technology Services (IITS) to secure credit card holder systems and credit card holder data, in any media, by:

- maintaining a secure network;
- changing default system passwords on any networking equipment and using strong encryption for the authentication and the transmission of data;
- removing any unneeded services or protocols from credit card systems;
- providing encrypted access to non-console administrative systems;
- taking proper technical measures to ensure that sensitive credit card holder data is not stored when it is not required;
- ensuring that anti-virus software is installed and kept up-to-date on all University's systems used for credit card transactions;
- ensuring that all critical patches are applied on all University's systems used for credit card transactions;
- taking measures to restrict physical access to any University's credit card systems and University's media containing credit card holder data;
- regularly testing security systems and processes;
- ensuring that a unique ID is provided to all Authorized Users;
- mapping and monitoring the usage and devices of Authorized Users;

- taking measures to ensure the automatic disconnecting of sessions for remote-access technologies;
- establishing, documenting, and distributing IT Incident responses and escalation procedures to ensure the timely and effective handling of all security incidents;
- reporting every IT Incident to Financial Services as described in IT Incident reporting procedure emitted by Financial Services.

6. It is the responsibility of the Authorized Users to secure credit card systems and credit card holder data, on any media, by:

- adhering to the Policy, to any measures and Guidelines provided by Financial Services;
- assisting in the incident response procedures within their particular areas of responsibility.