Carleton
UNIVERSITY
Canada's Capital University

Policy Name:	Cardholder Data Network Policy
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Chief Information Officer (CIO)
Date of Original Policy:	April 5, 2013
Last Updated:	September 2015
Mandatory Revision Date:	September 2016
Contact:	Director, Information Security, ITS

Policy:

As part of Payment Card Industry (PCI) compliance, ITS maintains a proprietary network for the purposes of connecting systems and devices used to process credit card cardholder data. This cardholder data network will adhere to the security standards as described in the Payment Card Industry Data Security Standard.

Purpose:

The purpose of this Policy is to define the security parameters governing the management of the cardholder data network at Carleton University.

Scope:

This Policy applies specifically to the systems within the scope of the cardholder data network.

Procedures:

1.0 Firewalls

Firewalls are used to restrict network traffic in and out of the cardholder data network. The following firewall policy requirements exist:

- Only network traffic required for the proper functioning of devices within the cardholder data network is permitted
- Network traffic to and from the Internet must traverse network firewalls - there is no direct communication from devices in the cardholder data network to and from the Internet
- Devices in the cardholder data network employ Network Address Translation (NAT) for access to external networks
- Remote access to the cardholder data network from off campus must follow the procedures outlined in the Remote Network Access Policy
- All other network traffic will be explicitly denied

- The firewall rules controlling access to the cardholder data network must be reviewed every six months by ITS Information Security – ITS must also scan to detect and identify both authorized and unauthorized wireless access points on a quarterly basis

1.1 Changes to Firewall Configurations

Updates to the firewall rules controlling access to the cardholder data network must follow a formal process. In addition, the following requirements must be met:

- Any change to firewall and router configurations must be tested
- The impact of the change must be documented
- Functionality testing must be performed to verify that the change does not adversely impact security
- Back-out procedures must be documented

2.0 Remote Network Access

For remote network access procedures and requirements, refer to the Remote Network Access Policy.

3.0 Public Access Areas

Network jacks in public areas with access to the cardholder data network must be:

- Disabled when not in use
- Only enabled when network access is explicitly authorized by the Information Security Group
- Physically protected from unauthorized access

Cellular point of sale terminals must be used for non-permanent locations.

4.0 Point of Sale (POS) Terminal Provisioning and De-provisioning

A formal process must exist for the provisioning and decommissioning of PCI services. This process must:

- Capture network jack information for deployed POS terminals
- Ensure that network jacks are disabled when POS terminals are decommissioned

Roles and Responsibilities:

ITS is responsible for:

- Every six months, reviewing the configuration of access rules which control access to the Cardholder Data Network
- Conducting quarterly scans to detect and identify both authorized and unauthorized wireless access points
- Adhering to the Business Office POS Terminal Process Flow

The Business Office is responsible for:

- Ensuring the physical security of POS terminal locations meets PCI DSS requirements
- Maintaining and adhering to the Business Office POS Terminal Process Flow

Merchants are responsible for:

- Ensuring that only authorized access to POS network jacks is permitted

Compliance:
Non-compliance with this Policy may result in disciplinary action.

Contacts:
Assistant Director, Information Security, ITS

Links to Related Policies:

- ITS Policies (http://carleton.ca/its/about-its/policies/)
  - ITS Change Management Policy
- Secretariat Policies (http://carleton.ca/secretariat/policies/)
  - Acceptable Use Policy for Information Technology (IT)
  - Remote Network Access Policy
  - Information Technology (IT) Security
  - University e-Commerce Policy
- Financial Services
  - Cardholder Data Handling Policy