BRANDON UNIVERSITY	**PCI –DSS (Payment Card Industry – Data Security Standards) Policy**	***Approved by*** *PAC* ***Administered by*** *Administration & Finance*
Administrative Policy	***First Approved:*** *February 5, 2015*	***Updated:*** *May 11, 2016, September 11, 2019*

Preamble

PCI DSS (Payment card Industry Data Security Standards) is a global initiative for the purpose of securing credit and banking transactions through an evolving set of mandatory operational and technical requirements and guidelines covering security, policies, procedures, network/software design and other critical protective measures. All card processing activities and related technologies must comply with the PCI-DSS Policy in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Scope

This policy is applicable to all University staff members with access to cardholder information and departments who accept cards for payment by whatever means:

- Internet (gateway provider)
- Face to face (point of sale terminals)
- Non face to face (information provided via phone)

PCI Security Standards Council Data Security Standards

Build and maintain a secure network and systems:

Configuration standards must be maintained for applications, network components, critical servers, and wireless access points. Configuration standards must include but are not limited to:

- Ensuring anti-virus and malware mechanisms are actively running and updated
- provision for installation of all relevant new security patches within one month.
- prohibition of group and shared passwords.
- Implementing strong cryptography

- Ensuring vendor supplied defaults are removed or amended

Protect cardholder data:

Distribution, maintenance, and storage of media containing cardholder data, must be controlled at all times.

Procedures for data retention and disposal are as follows:

- no cardholder data is to be stored by the University unless it is necessary to meet the needs of University business.
- cardholder data is not stored in electronic format at any time
- cardholder data, when no longer needed for business reasons, is to be deleted or rendered unrecoverable. Destruction of hardcopy materials is to be cross-shred.
- cardholder data, if required to be stored, will be stored in the vault in Financial & Registration Services in a container marked confidential. A log will be used to record when the container is signed out and signed back in.
- for room deposits, casual accommodations and conference bookings; Ancillary Services will store credit card information until the booking is confirmed & payment can be completed.
    - cardholder data, if required to be stored, will be stored in the vault in Ancillary Services in a container marked confidential. A log will be used to record when the container is signed out and signed back in.
- credit card numbers will not be displayed on client receipts.
- unencrypted Primary Account Numbers may not be sent via email or facsimile.
- no pictures via cell phones are to be taken of cardholder data, nor duplication by any means.

Procedures for data control are as follows:

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities.
- Assignment of privileges is based on individual personnel's job classification and function.
- Requirement for an authorization form signed by management that specifies required privileges.

Critical Employee Facing Technologies:

For critical employee-facing technologies (inclusive of remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and personal data/digital assistants), departmental procedures shall require:

- explicit management approval to use the devices during face to face transactions.
- that all device use is authenticated with username and password.
- a list of all devices and personnel authorized to use the devices. Additionally, a list will be maintained of all staff devices (cell phones) that may be used for duplication purposes, by name only.
- that only University owned and approved equipment is authorized to process payment card transactions.

Departmental usage standards shall include:

- acceptable uses for the technology.
- acceptable network locations for the technology.
- prohibition of replacing or adding devices without the authorization of Financial & Registration Services.
- prohibition of the storage of cardholder data onto local hard and, or networked drives and removable electronic media.

Roles and Responsibilities

Information Technology Services is responsible for overseeing all aspects of information security, including but not limited to:

- creating and distributing security policies and procedures.
- monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
- creating and distributing security incident response and escalation procedures that include:
    - roles, responsibilities, and communication.
    - coverage and responses for all critical system components.
    - notification, at a minimum, of credit card associations and acquirers.

- monitor for intrusion detection and prevention on a 24/7 basis.
- plans for periodic training.
- a process for evolving the incident response plan and mitigation plan according to lessons learned and in response to industry developments.

The Information Technology Services shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS as follows:

- monitor and analyze security alerts and information and report as required.
- administer user accounts and manage authentication.
- control all access to data.
- retain audit logs for at least one year.

Financial & Registration Services is responsible for tracking employee participation in the security awareness program, including:

- facilitating participation upon hire and at least annually.
- ensuring employees acknowledge in writing at least annually that they have read and understand the information security policy.

Financial & Registration Services shall maintain daily administrative responsibility to:

- maintain a list of service providers.
- ensure there is a process for engaging service providers including proper due diligence prior to engagement.

- confirm service providers' PCI-DSS compliant status, with supporting documentation.
- maintain control and listing of all devices and associated passwords, whether new or replacements.