Policy

Title:	Cardholder Data Information Security Policy
Effective Date:	12/12/2017
Approved By:	President's Council
Responsible Party:	Chief Information Officer
History:	None
Related Documents: Use of Electronic Communications Policy	

I. PURPOSE

The University is committed to respecting the privacy of all its customers and to protecting any/all data about customers from outside parties. This policy provides guidelines for the handling of sensitive cardholder data and related data in order to secure sensitive data information from unauthorized or unlawful disclosure.

II. DEFINITIONS

CVV/CVC: Card Verification Value/Card Validation Code

PCI DSS: Payment Card Industry Data Security Standard. The standard that promotes the safety of cardholder data implemented for protection of their payments systems enabling secure solutions.

PAN: Primary Account Number

PIN: Personal Identification Number

Sensitive Data: Protected Health Information, Social Security Numbers, Cardholder Data Numbers, Financial Account Numbers, and other information protected by HIPAA, FERPA, and other laws and regulations.

III. POLICY

The University will have adequate safeguards in place to protect cardholder privacy and to ensure compliance with various regulations as it relates to Sensitive Data. All those associated with the University who handle cardholder data information must take the precautions listed herein.

a. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

b. Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
c. Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
d. Employees must keep passwords secure and not share accounts.
e. Authorized users are responsible for the security of their passwords and accounts.
f. All PCs, laptops and workstations should be secured with a password-protected screensaver.
g. All PIN entry devices should be appropriately protected and secured so they cannot be tampered with or altered.

IV. PROCEDURE

Employees handling Sensitive cardholder data are required to:

a. Process University and cardholder information in a manner that fits with their sensitivity;
b. Ensure that personal information is not disclosed unless authorized;
c. Protect sensitive cardholder information;
d. Keep passwords and accounts secure;
e. Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
f. Always leave desks clear of sensitive cardholder data and lock computer screens when unattended.
g. Report information security incidents without delay to the Director of Network Security Services.

Protect Stored Data

a. All sensitive cardholder data stored and handled by the University and its employees must be securely protected against unauthorized use at all times. Any sensitive card data that is no longer required by The University for business reasons must be discarded in a secure and irrecoverable manner. The contact for this procedure would be the Director of Network Security Services.
b. If there is no specific need to see the full PAN (Primary Account Number), it has to be masked when displayed.
c. PANs which are not protected as stated above should not be sent outside of the network.
d. It is strictly prohibited to store:
    i. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
    ii. The CVV/CVC (the 3- or 4-digit number either on the front of the payment card or on the reverse side next to the signature panel) on any media whatsoever.
    iii. The PIN or the encrypted PIN Block under any circumstance.

Access to sensitive cardholder data

a. Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.

b. Any display of the cardholder should be restricted to the last 4 digits only of the cardholder data.
    i. Privileges for a and b above should be assigned to individuals based on job classification and function.
c. If cardholder data is shared with a Service Provider (3rd party), then a list of such Service Providers will be maintained by the Director of Network Security Services.

Physical Security

a. Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies. TLS provides a list for this purpose.
b. Employees should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.
c. TLS will maintain a list of devices that accept payment card data. Such list will be update as needed.
    i. The list should include: make, model and location of the device.
    ii. The list should have the serial number or a unique identifier of the device.
    iii. The list should be updated when devices are added, removed or relocated.
    iv. Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
d. Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
e. Cardholder data, including PANs, are not to be stored electronically on the network or other media.

Protect Data in Transit

a. Sending cardholder data (PAN, track data etc.) over the internet; via email, instant chat or any other end user technologies is strictly prohibited unless properly protected.
b. If there is a business justification to send cardholder data via email or via the internet or any other modes, then it may only be done after authorization and by using a strong encryption mechanism.

Disposal of Stored Data

a. All data must be securely disposed of when no longer required by the University, regardless of the media or application type on which it is stored.
b. All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been

appropriately disposed of in a timely manner. Department heads are responsible for ensuring this process occurs.

c. Hard copy (paper) materials containing sensitive data must be destroyed by being crosscut shredded, incinerated or pulped so they cannot be reconstructed.
d. All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted. These containers are padlocked and can be located throughout campus buildings and clinics.

Security Awareness and Procedures

a. Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice. The Director of Network Security Services will conduct these reviews.
b. All third parties with access to cardholder data account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
c. Network security policies will be reviewed annually and updated as needed.

The University reserves the right to monitor, access, review, audit, copy, store or delete any electronic communications, equipment, systems and network traffic at any time.