**PCI-DSS Procedure**

# PurposeThe purpose of this procedure is to provide awareness that all credit card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures released by the Cybersecurity department. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

# Scope

# All staff, employees and entities working on behalf of the [Organization] are subject to this procedure.

# Procedure

Adherence to Standards
Configuration standards must be maintained for applications, network components, critical servers, wireless access points or any other equipment involved in the transaction process. These standards must be consistent with industry-accepted hardening standards as defined by organizations such as SysAdmin Assessment Network Security Network (SANS), National Institute of Standards and Technology (NIST) International Organization for Standardization (ISO) and Center for Internet Security (CIS.) Configuration standards must include:

* Updates to anti-virus software and definitions
* Performance of periodic scans
* Generation of audit logs
* Identification of new security vulnerabilities along with Risk Ranking assignments for all “High Risk” and “Critical” vulnerabilities
* Installation of all relevant security patches within 30 days of release
* Assignment of authentication mechanisms to individual accounts rather than shared accounts
* Implementation of physical and/or logical controls in order to ensure only the intended account can gain access

Handling of Cardholder Data

* Distribution, maintenance, and storage of media containing cardholder data, must be controlled, including that distributed to individuals.
* Procedures must include periodic media inventories in order to validate the effectiveness of these controls.
* Listings of devices must be maintained along with periodic inspections of devices for signs of tampering.
* Training mechanism must be placed to alert staff when device tampering is evident.
* Procedures for data retention and disposal must be maintained by each department and must include the following legal, regulatory and business requirements which include:
	+ Specific requirements for retention of cardholder data
	+ Provisions for disposal of data when no longer needed including disposal of cardholder data

Handling of Cardholder Data (cont.)

* + A process to remove stored cardholder data that exceeds business retention requirements (at least on a quarterly basis)
	+ An audit process to verify that stored cardholder data does not exceed business retention requirements (at least on a quarterly basis)
	+ Destruction of media leveraging one of the following techniques: cross-cut shred, incinerate or pulp hardcopy materials. Purge, degauss, shred or otherwise destroy electronic media such that data cannot be reconstructed

Roles and Responsibilities

* Cybersecurity Officer (or equivalent) 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
	+ Monitoring service providers PCI compliance at least annually
	+ Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (e.g. posters, letters, meetings)
	+ Reviewing daily security logs and follow-up on noted concerns
* The Information Technology Office (or equivalent) should maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (e.g. user account maintenance procedures and log review procedures.)
* System and Applications Administrators should:
	+ Monitor and analyze security alerts and/or information and then distribute to appropriate personnel
	+ Administer user accounts and manage authentication
	+ Monitor and control all access to data
	+ Maintain a list of connected devices
	+ Perform due diligence prior to connecting a device including supporting documentation

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

The Network Services and/or Cybersecurity teams will verify compliance with these procedures through various methods, including but not limited to: period walk-throughs, business tool reports, internal and external audits, and feedback to the procedure owner.

# Exceptions

Limited exceptions to the procedure must be approved by the **[management].**

1. **Definitions**
* Not applicable at this time.