Controls for the Credit Card Environment
Edit Date: May 17, 2007

Status: Approved in concept by Executive Staff 5/15/07

This document contains policies, standards, and procedures for securing all credit card information within the University.

I. Definitions:

CC: Credit Card data, including, but not limited to, 16-digit account number and expiration date
CCE: Credit Card Environment, all the electronic and non-electronic systems and mechanisms for receiving, processing, storing, and transmitting CC data
ITS: The Division of Information Technology Services
VPN: Virtual Private Network or similar technology for encrypted access

II. Scope:

CC data in all forms, both electronic and non-electronic

III.A. Policy: Oversight

1. Responsible Authority. The office responsible for oversight of all Credit Card data and uses. The Office of the Treasurer is the Responsible Authority. The Division of ITS, as well as other divisions of the University, will assist the Responsible Authority in carrying out these responsibilities.

2. The Responsible Authority is responsible for evaluating the CCE to ensure compliance with applicable standards and regulations. It is the responsibility of ITS and any other division that is responsible for any component of the CCE to report to the Responsible Authority regarding status and changes to University compliance with all applicable policies or standards related to the CCE.

3. The Responsible Authority is ultimately responsible for monitoring and controlling all access to CC data.

4. The Responsible Authority is responsible for the establishment, documentation, and distribution of relevant policies and procedures.

5. The Responsible Authority is responsible for maintaining a current list of administrators for each CCE element.

6. The Vulnerability Oversight Committee (VOC) is responsible for analyzing security alerts and information, and distribute to appropriate personnel.

7. The VOC is responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
8. The administrator of each CCE element is responsible for ensuring that there is an effective backup and recovery procedures for each system component. In the event that a component is at risk of an insufficient recovery, it is the responsibility of the administrator to report that to the Responsible Authority.

9. At all times, ITS shall ensure that at least one (1) person listed on the University’s Emergency Contact List is available.

**B. Policy: Access Controls**

1. The standard for access control is the “need to know” standard.

2. Each account shall be a unique identifier for each user.

3. No group, shared, or generic accounts are allowed.

**C. Policy: Application Development**

No applications may be developed internally to process or handle credit card data. This prohibition includes all web, server, desktop, mobile, and other applications.

**D. Policy: Data and Data Retention**

1. Storage and retention of CC data shall be the minimum amount and duration necessary for operational, legal, and/or regulatory purposes. The Responsible Authority is solely responsible for approving the storage and retention schedule for each CCE, and the administrator of each process involving CC data shall abide by the Responsible Authority’s decision. No CC data may be collected, processed, or stored without approval.

2. The following information may not be retained in any database, log, or within any point-of-sale device:
   - discretionary data/CVV
   - the full contents of any track
   - the PIN verification value.

3. The display of CC information shall be limited to the last four digits unless specifically approved by the Responsible Authority as a legitimate business need.

4. Stored CC data in all media (including on-line, backups, logs, etc.) shall be rendered unreadable by one or more of the following methods:
   (a) One-way hashes (hashed indexes), such as SHA-1
   (b) Truncation
   (c) Index tokens and PADs, with the PADs being securely stored
   (d) Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.

   The MINIMUM account information that needs to be rendered unreadable is the payment card account number.

5. Sensitive data transmitted over public networks must be protected with strong cryptography and encryption techniques (at least 128 bit), such as SSL, (Secure Sockets Layer), PPTP (Point-to-Point Tunneling Protocol), or IPSEC (Internet Protocol Security).
6. Cardholder data may not be sent via unencrypted e-mail.

7. All passwords must be encrypted during transmission and storage.

8. All media containing cardholder data must be secured against unauthorized removal, tampering, and viewing. This includes, but is not limited to:
   - computers
   - electronic media (e.g., tape, disk, flash drive)
   - networking and communications hardware
   - telecommunication lines
   - paper receipts
   - paper reports
   - faxes

9. Movement or distribution or a standard procedure for movement or distribution of any media containing cardholder data must be approved in advance by the Responsible Authority.

10. Media containing cardholder data removed from secure facilities must have prior approval by the Responsible Authority.

11. Media containing cardholder data must be labeled as ‘confidential’.

12. Media may be sent only by a carrier and means approved by the Responsible Authority. Carrier must have security, and movement must be tracked.

13. The Responsible Authority or his/her designee shall perform an inventory of all media at least once per year. The review must include an evaluation of the adequacy of the security of the stored data.

14. The process of media must be secure. For electronic media, the ITS standard for media shall be followed. For hardcopy materials, they can be either cross-cut shred, incinerated, or pulped.

E. **Policy: Key Management**

There shall be no generation, storage, or handling of encryption keys.

F. **Policy: Review**

1. At least once per 12-month period, the Responsible Authority shall ensure that a review of CC security is performed.

2. At least once per 12-month period, the Responsible Authority, with the assistance of ITS, shall ensure that a risk assessment is performed to identify threats and vulnerabilities.
G. Policy: Third-Party Access

1. Third parties with access to cardholder data must be contractually obligated to comply with the payment card industry security requirements. At a minimum, the contract should include:
   - the third party is responsible for security of the cardholder data that is in their possession
   - ownership and acceptable uses of the data for specific purposes
   - business continuity in the event of a major disruption, disaster or failure
   - audit provisions that ensure that an approved representative of the Payment Card Industry will be provided with full cooperation and access in the event of a security intrusion in order to conduct a security review
   - a termination provision to ensure the continued treatment of cardholder data as confidential

2. The third-party is responsible for providing documentation of their compliance level.

H. Policy: Wireless/Remote

1. Mobile devices are not allowed within the CC environment.

2. Cardholder data may not be transmitted over wireless connections; wireless devices may not be incorporated into the CCE.

3. Modems and modem types (brand, model) may be used to access CCE with explicit approval by the Responsible Authority, and use is limited to only those uses and locations which are approved. The Responsible Authority will maintain a list of devices, device types, and those with access. Modem access must include authentication. Modems must be labeled with owner, contact information, and purpose. Modem must be configured to disconnect after an inactivity period of 15 minutes or less.

4. When a user is accessing cardholder data remotely, all local storage and retention mechanisms (e.g. saving to hard drive, flash drive, copy/paste, printing) are prohibited.

5. Remote access to CCE is only allowed with 2-factor authentication using either the VPN with individual certificates, RADIUS, or TACACS.

IV.A. Standard: Access

1. Administrative access to servers (non-console) must be encrypted using SSH (Secure Shell), VPN, or SSL/TLS (Secure Socket Layer, Transport Layer Security) for web-based access.

2. For systems with multiple users, access must be restricted based on each user's need to know, and set to "deny all" unless specifically allowed.

3. Authentication of access control may use one or more of the following, in combination with a username:
   - password
   - token device
   - biometric
4. Management of accounts and passwords (including additions, deletions, and modifications) is performed by the security administrator for each CCE component (system).

5. Access methods (including modems) for vendor remote maintenance/support must be enabled only when the access is needed.

6. Failed access attempts of 6 shall result in a lock-out of the account. Lockout duration may be a period of time of at least 30 minutes, or until an administrator intervenes.

7. Each session shall be subject to a 15-minute time-out period; if there is no activity for a period of 15 minutes, the user must enter the password in order to resume the session.

8. Access to all storage containing cardholder information must be authenticated. This includes access by administrators, applications, and other users.

B. Standard: Anti-virus

1. All workstations and LAN servers must run current anti-virus defenses.

2. Production systems must have anti-virus mechanisms running at all times with current threat information. The anti-virus mechanism must be capable of generating audit logs.

C. Standard: Audit Trail

1. All system components must have an automated audit trail. The audit trail must contain information sufficient to reconstruct the following events:
   - All individual accesses to cardholder data
   - All actions taken by any individual with root or administrative privileges
   - Access to all audit trails
   - Invalid logical access attempts
   - Use of identification and authentication mechanisms
   - Initialization of the audit logs
   - Creation and deletion of system-level objects

2. The audit trail must contain the following fields for all system components:
   - User identification
   - Type of event
   - Time stamp (date and time)
   - Success/Fail indication
   - Origination of event
   - Identity or name of affected data, component, or resource

3. All system clocks must be synchronized.

4. The integrity of the audit trail information must be maintained. Viewing of the audit trails is limited to those with a job-related need. Modifications can only be made by those with specific authorization. Audit trail information must be sent to the centralized correlation system or backed up to a media that is difficult to alter.

5. Integrity of audit trail logs must be monitored, and alerts generated for changes.
6. The centralized correlation system shall include systems that perform intrusion detection and authentication functions. The correlation system must review input promptly with a maximum delay of 24 hours from input to review.

7. The audit trail history shall be retained for at least one year, with at least three (3) months available on-line.

D. **Standard: Firewall**

1. Changes to the firewall configuration must be tested and approved through the change control procedure.

2. There shall be a firewall between the CCE and the Internet.

3. All connections, both inbound and outbound, between publicly-accessible servers (including the wireless network) and the CC environment are blocked. Outbound traffic must be restricted to only that which is necessary.

4. There shall be no public access to or from any host containing CC data.

5. Routers settings and changes that support, modify, or influence the effectiveness of firewalls must be included in the firewall standard and in its change control process.

6. Router configuration files must be synchronized and secured so that start-up configuration files are consistent and secure.

7. The firewall must use stateful inspection.

8. The CC data must be on an internal network zone.

9. Current diagram of network paths to CCE must be maintained by ITS.

10. The firewall rule sets must be reviewed at least every three (3) months.

11. Responsibility rests solely on ITS Network Services for the operation and management of all CCE network components.

12. The Responsible Authority shall maintain the list of necessary services/ports, which will be provided by ITS Network Services. The list must include for each service/port the network area and the business requirement.

13. The Responsible Authority shall maintain the list of protocols (other than HTTP, SSL, SSH, and VPN) that are allowed, along with the justification and security features of each:

14. The firewall must block any traffic not specifically allowed (“deny all” rule).

15. All traffic from “untrusted” networks/hosts is denied unless specifically allowed and documented.
E. Standard: Physical Facilities and Access

1. There are three types of physical areas within the CCE
   Type 1: Electronic information processing with single-card handling (such as swipe devices, cash registers, etc.)
   Type 2: Electronic information systems and storage
   Type 3: Electronic information storage (with no processing) (such as storage of backup tape)
   Type 4: Non-electronic information processing and storage
   Type 5: Non-electronic information storage (with no processing)

Some locations may have a combination of types; each area must comply with the standards for each type of information contained therein.

2. All facility types containing cardholder data must have limited access.

3. Type 2 areas must be monitored through cameras; video information must be stored for at least 3 (three) months.

4. Type 2 areas must use visitor logs to record all visitor access. The logs must be retained at least three (3) months.

5. Type 3 areas must be secured against access by unauthorized individuals.

6. Type 4 and Type 5 areas must use locked containers or areas with limited access. The storage and access control information must be reported to the Responsible Authority at least once per year and whenever changes are considered or made.

7. Network jacks that have access to the CCE shall not be accessible to the public.

F. Standard: Staff Selection

1. All employees and contractors (staff and faculty) with access to the CCE must pass the background check process successfully before being given access to CC data or functions.

2. Employees and contractors (staff and faculty) with access to the CCE must sign an agreement verifying they have read and understand the applicable security policies, standards, and procedures before being given access to CC data or functions.

G. Standard: System and Network Configuration

1. All system components must be configured to a documented ITS standard. The standards must ensure that:
   - Each server has only one primary function
   - Unnecessary services and protocols are disabled
   - Misuse is prevented
   - Unnecessary functionality, such as scripts, drivers, features, sub-systems, file systems, etc. is removed

2. Network configuration of routers, switches, firewalls, and wireless access points must at a minimum be configured to the following standards:
3. The network shall be designed and implemented with the following conditions, unless given an exemption by the Responsible Authority:
- no publicly accessible web services for CC handling
- devices that store CC data must use private addressing according to RFC 1918 (e.g. Network Address Translation or Port Address Translation)

4. When installing a system on the network, the security hardening steps must include:
   - change vendor default passwords
   - remove unnecessary accounts
   - SNMP community strings

**V.A. Procedure: Accounts**

1. Terminated users must have access revoked immediately; it is encouraged to revoke access when it is first learned that the individual is clearly intending to leave (at time that notice is given).

2. All accounts must be reviewed every 30 days. Any user account (other than administration and support) that has been inactive for more than 90 days must be removed from the system. Accounts that are by nature used infrequently, such as administration and support accounts may remain idle for 180 days before removal.

3. Accounts for vendors for remote maintenance must be disabled when not in use.

**B. Procedure: Change Control**

1. Changes to the firewall configuration must be tested and then approved by the ITS Change Control Board before implementation. In the event than an emergency change is necessary, the change must pass the approval process as soon as practicable in order to remain in production. The Responsible Authority may at any time review past change decisions, prohibit changes that are inconsistent with standards of compliance or security, and/or require additional prior review of changes.

2. Scope of the Change Control process includes, at a minimum, all changes in:
   - the network core
   - network security, shaping, or filtering (IDS, Packeteer, firewall, &c.)
   - servers within the CCE
   - all applications on each servers within the CCE

3. In order for a change to be approved, it must have
   - Documented assessment of impact
   - Documentation of testing that verifies operational functionality
   - Documented back-out procedure
- sign-off (active) to indicate the receipt of information about the change, an opportunity to approve, deny, and request additional information
- sign-off (active) by
  o the lowest ITS management position that is in charge of any aspect of the change (e.g., when the change is exclusively networking, the manager of networking must approve; when the change is networking and servers, the management over both networking and servers must approve)
  o the management of non-ITS areas that may be affected by the change (e.g., a change that may affect Parking & Card Services systems must be approved by Parking & Card Services management)
  o Security Review Committee

4. Penetration testing must be performed after any significant infrastructure upgrade or modification has been implemented.

C. Procedure: Incident Response

1. Refer to the Information Security policy for roles and responsibilities for incident response or contact the Information Security Officer.

2. In the event that there is a system compromise involving cardholder data, the Incident Response Team shall notify the Responsible Authority. The Responsible Authority will notify the appropriate financial institutions.

D. Procedure: Password

1. Password resets shall only be performed after in-person identity verification, or for situations were in-person verification is not practical such as remote vendor support, multiple reliable forms of identification must be presented and verified.

2. The appointment of each administrator of accounts and access must be approved by the Responsible Authority.

3. Password reset requests must include verification of identity.

4. Initial password must be unique for that user. First use must require password change.

5. Passwords must be changed at least every 90 days.

6. A password history of at least four (4) is required without repeating.

7. Passwords must have complexity requirements:
   - seven character minimum
   - containing both numeric and alphabetic characters

E. Procedure: Patching

1. The process for keeping all CCE devices (systems and network devices) current on patch levels includes the following steps:
   - Each system administrator must be registered to receive prompt notification of the release of each patch
- The system administrator evaluates the applicability of the patch
- The system administrator verifies the source and integrity of the patch
- The system administrator tests the patch
- The system administrator coordinates approval and scheduling for installation of the patch
- The system administrator implements the patch

2. Time frame for patch installation:
   - Security: one month of release

3. The system administrator for each CCE component shall monitor for newly discovered vulnerabilities. Proposals for updating standards in response to vulnerabilities shall be submitted to the Responsible Authority for consideration.

F. Procedure: Physical Access

1. All visitors to areas of stored CC information (Types 2, 3, 4 and 5) shall be escorted at all times by an employee with legitimate access. Visitors are those who are not one of the following: employees, temporary employees/personnel, consultants, or contractors with legitimate, routine, need-to-know access.

2. It is the responsibility of the visitor escort to ensure that
   - the visitor is authorized by the unit responsible for the area to access the area
   - the visitor is given and displays a temporary, numbered badge that identifies them as a visitor
   - the visitor surrenders the temporary badge at the end of the visit
   - the visit is logged

G. Procedure: Review

The Firewall rule sets will be reviewed at least once every three (3) months. The Information Security Officer or his/her designee will perform and document the review to ensure that all settings are in compliance with standards and good practice.

H. Procedure: Testing

1. At least every three (3) months, ITS shall perform or oversee an internal vulnerability scan of CCE components in order to identify vulnerabilities and verify controls.

2. At least once per year, ITS shall perform or oversee a penetration test on the network infrastructure and applications.

I. Procedure: Training Content and Means

1. Training of individuals involved in operating and supporting the CCE will include the importance of security of CC data.

2. Password procedures and policies are to be made available to all users with access.

3. Training should educate users through various means, such as meetings, posters, memos, meetings, and promotions.