Cardholder Data Environment Policies

Table of Contents

Cardholder Data Environment
Credit Card Acceptance Policy

I. POLICY STATEMENT

Departments or units must contact the Office of Cash Management to begin the process of accepting credit cards or to modify an existing merchant account. Any department or unit accepting credit cards on behalf of the Auburn University System or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions. Approval of new merchant accounts shall be at the discretion of the Office of Cash Management in conjunction with the E-Commerce Committee Any fees associated with the acceptance of credit or debit cards will be charged to the accepting unit. All approved merchants must remain compliant with the Payment Card Industry – Data Security Standards (PCI-DSS) and validate such compliance on an annual basis and must also adhere to any Auburn University Business Office Policies or required procedures including all Auburn University Cardholder Data Environment policies. The Office of Cash Management, together with the Office of Information Technology, shall determine acceptable hardware/software utilized to process credit cards.

II. POLICY PRINCIPLES

The Office of Cash Management is part of the Auburn University Business Office and oversees the operational cash flows of the University to provide liquidity with maximum return within the guidelines of AU policy. Cash Management is also charged with management of the Merchant Credit Card Program for the University and affiliated foundations. Auburn University is contractually obligated by the payment card brands and our acquiring bank to adherence of the PCI-DSS. The Office of Cash Management is therefore charged with overseeing all activities related to payment card acceptance.

III. EFFECTIVE DATE

March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, students, contractors, consultants, temporary, and other workers collecting credit or debit card payments on behalf of the Auburn University system or related foundations.

V. POLICY MANAGEMENT

Responsible Office: Office of Cash Management
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Interested departments or units should refer to the Credit Card Merchant Procedures Manual (available from the Office of Cash Management) to learn more about becoming a merchant and day-to-day merchant procedural requirements.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management.

ADOPTED: March 18, 2014
REVISED: March 1, 2015

Cardholder Data Environment
User Authentication and Access Policy

I. POLICY STATEMENT

Authentication and access control to the Auburn University Card Holder Data Environment will be implemented in such a manner to (at a minimum) ensure compliance with the provisions of the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 Identification

To ensure proper user identification and authorization:

- **1.1.1** User accounts must use a unique identifier, no group or sharing accounts are permitted, vendor and service provider accounts shall be issued only to individual users.
- **1.1.2** User identity must be verified prior to account creation or performing password reset requests
- **1.1.3** Users must annually acknowledge understanding of this policy and related procedures.
- **1.1.4** Accounts must conform to the following parameters.
  - **1.1.4.1** First time passwords must be unique and changed upon first use
  - **1.1.4.2** Passwords must change every 90 days
  - **1.1.4.3** Group or shared passwords must not be utilized
  - **1.1.4.4** Passwords must be at least 8 characters and use a combination of upper-case, lower-case, numeric and special characters.
  - **1.1.4.5** User passwords cannot be the same as any of the last 4 used by that user
  - **1.1.4.6** Accounts must utilize at least a 30 minute lockout when login failure attempts exceed 6.
  - **1.1.4.7** Passwords must be rendered unreadable and utilize strong cryptography during transmission and on any storage system.
- **1.1.5** System access must be logged. Success and failure access to all system data must be logged and retained for at least 1-year. Logs must be kept online and available for 90 days. Additional system logging policies are located in the Auburn University PCI-DSS Logging Control Policy.
- **1.1.6** Sessions which have been idle for more than 15 minutes must require the user to re-authenticate to re-activate the terminal or session. Remote sessions must be disconnected after 15 minutes of inactivity.
- **1.1.7** All computers used to process payments on behalf of others or to access cardholder data must be connected to a PCI compliant network with internet access limited to only those sites necessary for completing the payment process.
- **1.1.8** Two-factor authentication technologies are required for remote access (network-level access originating from outside the CDE network) to the CDE network by non-consumers. Second-factor mechanisms (e.g. token, smart-cards or certificates) must be linked to individual accounts to ensure only the intended user may gain access with that mechanism.
- **1.1.9** Vendor accounts must only be enabled during the time that they are needed.
- **1.1.10** When vendor accounts are enabled, activity must be logged as required in the CDE Logging Control Policy.

1.2 Access

1.2.1 Access must be restricted based on an individual's job function and to data on a "need to know" basis.

1.2.2 All access to applications or devices within the CDE must be authorized and documented utilizing a management approved form.

1.2.3 A role-based automated access control system must be in place.

1.2.4 When accessing cardholder data through remote technologies (e.g. RDP), copying, moving or storing of cardholder onto local hard drives and other removable digital media is prohibited.

1.3 Removal

1.3.1 A process must exist to immediately disable and remove accounts that are no longer needed.

1.3.2 User Accounts must be reviewed; inactive accounts shall be retired at least every 90 days.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of CIO
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units.
Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

ADOPTED: October 15, 2012
REVISED: March 18, 2014
REVISED: March 1, 2015

Cardholder Data Environment
Acceptable Computer Use Policy

I. POLICY STATEMENT

Computer use within the Auburn University Card Holder Data Environment will be regulated in such a manner to (at a minimum) ensure compliance with the provisions of the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1. General Use and Ownership

1.1.1. All users are to adhere to this policy at all times when utilizing all network resources.

1.1.2. For security and network maintenance purposes, authorized individuals within the Office of Information Technology may monitor equipment, systems and network traffic at any time.

1.1.3. The Offices of Information Technology and Internal Audit reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy and associated policies.

1.2. Security and Proprietary Information

1.2.1. Only products (including hardware and software) approved by the Office of Cash Management and Office of the CIO for the transmission, processing and storage of cardholder data shall be utilized in the CDE.

1.2.2. The Office of Information Technology and the Office of Cash Management shall maintain an inventory of CDE system components that are in-scope for PCI-DSS to include both hardware as well as installed software.

1.2.3. A list of approved network locations for the transmission, processing and storage of cardholder data shall be maintained by the Office of Information Technology

1.2.4. Prohibit copy, move or storage of cardholder data to unauthorized systems when accessed remotely.

1.2.5. Vendor access to systems shall only be enabled when needed and immediately disabled after use.

1.2.6. Never send encrypted or un-encrypted Primary Account Number (PAN) through end-user messaging systems such as email, Short Message Service (SMS) or Instant messaging (IM)

1.2.7. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords shall be changed every 90 days.

1.2.8. All PCs, laptops and workstations that have security logging capabilities must have basic OS level auditing turned on to facilitate tracking of user accounts in the event of a security breach or other unauthorized access.

1.2.9. All systems commonly affected by malicious software shall continually execute approved virus-scanning software with a current virus signature list.

1.2.10. Management approval must be attained prior to use of any technology asset which connects to the CDE. A list of approved assets and users must be retained and reviewed annually.

1.3. Unacceptable Use

The following activities are prohibited on devices connected to the CDE. Employees may be exempted from these restrictions during the course of their legitimate job

responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Auburn University CDE resources. The list of prohibited activities presented below is by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use on the CDE.

1.3.1.1. Prohibited System and Network Activities - The following activities are strictly prohibited:

1.3.1.2. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

1.3.1.3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Auburn University does not have an active license is strictly prohibited.

1.3.1.4. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws.

1.3.1.5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, malware, etc.).

1.3.1.6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

1.3.1.7. Using an Auburn University CDE computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

1.3.1.8. Network monitoring for the purpose of malicious activity is expressly prohibited.

1.3.1.9. Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

1.3.1.10. Attempts to bypass the “in place” security measures dictated by this and other Auburn University policies.

1.3.1.11. Installing non-approved software onto CDE computers.

1.4. Management Approval to Use Technology

Auburn University requires management approval for the use of any technology connected to the CDE environment. Management approval procedures shall be determined by the Office of Cash Management and the Office of the CIO, in consultation with OIT. Users wishing to connect any new device to the CDE environment must solicit approval from the Office of Cash Management.

1.5. List of Approved Products

Auburn University is the legal owner of all CDE technology resources purchased or leased with University funds. The overall responsibility for administering and overseeing these technology resources rests jointly with the Office of Information Technology (OIT) and the Distributed IT Providers. The Office of Cash Management shall maintain a list of Auburn University-approved CDE technologies that may be used within the CDE.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
Physical Security Policy

I. POLICY STATEMENT

The Physical security surrounding equipment contained within the Auburn University Card Holder Data Environment will be regulated in such a manner to (at a minimum) ensure compliance with the provisions of the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 Access
All equipment that is involved in the CDE must be maintained in a secure environment appropriate for the device. (E.g. Servers should be located in locked cabinets within data centers, POS devices should be properly secured behind locked doors after working hours, paper containing cardholder data should be stored in locked drawers or safes when not in use, etc.)

1.2 All equipment that is connected to the CDE must have an affixed asset tag that maps the equipment to an inventory control list.

1.3 Implicit management approval must be granted for access to the data center(s) or other secure areas. Such access shall be based on individual job-function.

1.4 Individual authorization and access mechanisms to the data center(s) or other secure areas must be revoked immediately upon termination.

1.5 The data center(s) must limit access via badging, lock, or some other management approved security. Logs (electronic or paper) of ingress to the center must be maintained.

1.6 Authorized Personnel entering the data center or other secure areas, must be badged or easily distinguished from the public.

1.7 Visitors to the data center or secure areas must be badged or given some physical token that distinguishes them from employees and escorted by authorized employees at all times while in the secure area. The token must expire at a specific time and be surrendered at the time of departure from the facility.

1.8 Restrict physical access to network jacks, wireless access points, and routers. Unless in use, switch and router ports will be disabled or physically secured to prevent unauthorized connections.

1.9 Audit logs showing access to data center or other secure areas, must be retained for at least 1-year.

1.10 Physically secure all paper and electronic media that contains cardholder data. "Working documents" containing cardholder data must be stored in a safe or approved storage facility when not actively being used.

1.11 Equipment used for receiving or processing cardholder data must be secure when not in use.

1.12 Security

- **1.12.1** All sensitive and credit card data must be kept secure at all times.
- **1.12.2** Data centers must utilize man-traps, cameras, and electronic controls to protect devices and facilities.
- **1.12.3** Review of logs and camera systems shall be completed periodically and at least on a monthly basis.

1.13 Procedures must be in place and personnel trained to ensure device physical security. (Procedures must include, where applicable, a daily checklist for employees which includes checking for simple abnormalities e.g., a missing screw or seal, extra wiring, newly connected USB devices, etc.)

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
System Configuration & Application Hardening Policy

I. POLICY STATEMENT

A baseline security configuration for all hardware within the Auburn University Card Holder Data Environment and application hardening standards shall be established in such a manner to (at a minimum) ensure compliance with the provisions of the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 Documentation

1.1.1 Configurations of the network and systems involved in the CDE will be standardized and documented (e.g. build standards). Details shall include: Names, addressing, data flow and separation from non-CDE traffic. The following list of industry-leading security standards, benchmarks and frameworks to utilize in configuration of network and system components include, but is not limited to, the following:

- SANS (SysAdmin, Audit, Network ,Security) http://www.sans.org
- National Institute of Standards and Technology (NIST) http://www.nist.gov
- Center for Internet Security (CIS) http://www.cisecurity.org
- International Organization for Standardization (ISO)
- Vendor-specific tools and checklists, along with general setup and hardening procedures

1.1.2 Roles and responsibilities for logical management of network components shall be identified and documented. Roles include but not limited to: Security Admin, Network Admin, Approval admin, etc.

1.1.3 Enable only necessary and secure services, daemons, protocols and ports. All that are allowed must be documented with a business need for use, and documentation must be provided for use of insecure protocols such as FTP, TFTP, Telnet, SNMPv1, SNMPv2, POP3, IMAP, etc. including security measures afforded for their use. Secure protocols should be used whenever possible.

1.1.4 Remove all unnecessary functionality such as scripts, drivers, features, subsystems, file systems, default web pages and services.

1.1.5 A process for discovering new security vulnerabilities must be documented and defined configuration standards must be updated based on these discoveries.

1.2 General Configuration rules

1.2.1 When deploying or making modifications to system components, there is to be only one primary function per server so as not to require different security levels on any one given server. As such, all servers, both physical and virtual, will operate with one primary function only.

1.2.2 All default vendor passwords (and security related vendor defaults, e.g. SSID, SNMP community strings) must be changed prior to hardware or software being installed on the network.

1.2.3 System clocks on all equipment must be synchronized to a centralized time source that is synchronized to an external authoritative time source (e.g. time.nist.gov).

1.2.4 All transmission of sensitive card holder data over should be secured using strong cryptography and security protocols.

1.2.5 All remote console access shall be encrypted using standard strong encryption techniques. (Refer to CDE User Authentication and Access Policy for additional requirements for remote access.)

1.2.6 Configuration changes must be submitted to an authority for approval. Any changes must; be documented and dated, tested, and include rollback procedure.

1.2.7 File integrity monitoring software must be in place and setup properly on all systems within the CDE.

1.2.8 Security patches (including firmware updates) must be applied within one month of vendor release on all hardware platforms and software applications.

1.3 Firewalls

1.3.1 CDE networks will have a hardware based stateful packet inspection firewall installed at all Internet connections and between any non-CDE internal network (or DMZ.) Firewalls will be configured:

1.3.2 To deny all incoming traffic and will have exceptions based upon the specific business requirements of the CDE.

1.3.3 To deny all outgoing traffic and will have exceptions based upon the specific business requirements of the CDE.

1.3.4 To disallow any direct traffic between the CDE and Internet.

1.3.5 To allow management access from authorized workstations only specified by IP address.

1.3.6 Logging will be enabled and will log all incoming and outgoing connections. Logs will be maintained on a separate logging device within the CDE. Logs must be available for at least one year.

1.3.7 All CDE Firewall rule sets will be reviewed at least bi-annually.

1.3.8 Reviews must be documented and dated.

1.3.9 Running and startup configurations must be synchronized.

1.3.10 Anti-spoofing measures shall be implemented to detect and block forged source IP addresses from entering the network.

1.3.11 All configuration files must be secured to prevent unauthorized access.

1.4 Network Equipment

1.4.1 All networking equipment (switches, routers, IDS/IPS, etc.) will have default vendor passwords changed prior to being installed on the network.

1.4.2 All configuration files must be secured to prevent unauthorized access.

1.4.3 IDS/IPS will monitor all data at the perimeter of the CDE network and at all critical points inside the CDE network.

1.4.4 All connections to the CDE will be fully documented.

1.4.5 Active CDE network ports must be connected to an approved CDE device or physically secured to prevent non-CDE devices from connecting to the port, otherwise unused network ports should also be deactivated.

1.4.6 All requests for changes to the CDE must be documented and approved.

1.4.7 All devices will have logging enabled. Logs will be on a separate logging device. Logs must be available for at least 1 year.

1.4.8 All CDE equipment rule sets will be reviewed at least bi-annually.

1.4.9 Reviews must be documented and dated.

1.4.10 Running and startup configurations must be synchronized.

1.5 CDE Servers and Workstations

1.5.1 Servers and Workstations connected to the CDE will be installed and configured according to referenced industry best security practices (e.g. CIS, ISO, NIST, SANS).

1.5.2 Software installations will be limited to the approved software necessary for the operations of the CDE.

1.5.3 Workstations and servers must be configured based on the principle of least privilege.

1.5.4 Unnecessary protocols and services will be uninstalled, or made non-functional.

1.5.5 A host based firewall will be in operation and will deny all incoming traffic by default and will have exceptions for critical business functions only.

1.5.6 Sessions idle for 15 minutes shall require re-input of password to re-enable session.

1.5.7 Access to the system BIOS will be protected via a password mechanism where available.

1.5.8 Approved antivirus software will be installed, running, current and capable of providing audit logs at all times on all CDE machines that are currently susceptible to such compromises

1.5.9 For systems deemed *not currently affected* by malicious software, periodic evaluations should be conducted to determine the evolving malware threats against these systems, and where deemed appropriate, antivirus software shall be installed.

1.5.10 Antivirus software shall be installed such that end-users cannot disable or alter settings. Only specifically authorized administrators may change running configurations of antivirus software.

1.5.11 Device security logs will have their security logs forwarded to a secure server.

1.6 Vulnerability Assessments, Penetration Testing and Risk Assessments

1.6.1 Vulnerability scans will be completed quarterly on all systems in the CDE, internally by OIT and externally by a PCI approved scanning vendor.

1.6.2 Vulnerability scans (conducted internally by OIT or by a PCI approved scanning vendor) shall also be required after significant changes in the network topology and/or server configurations.

1.6.3 A process to identify and assign a risk ranking to newly discovered security vulnerabilities will be established by OIT.

1.6.4 Critical or Severe vulnerabilities will be addressed as soon as possible and within 30 days and systems re-scanned for complete remediation. Failure to remediate will result in server quarantine.

1.6.5 External penetration tests shall be completed on an annual basis (or requested by OIT, the CIO, or the Office of Cash Management) as required by PCI-DSS and should include testing of segmentation controls and methods. Exploitable vulnerabilities found during penetration testing must be remediated as soon as possible and within 30 days through patching or implementation of other controls and testing repeated to verify corrections.

1.6.6 A formalized risk-assessment process shall take place on an annual basis, and after significant changes to the CDE, to identify critical assets, potential threats and vulnerabilities.

1.6.7 Build standards will be reviewed and updated as needed when new high-risk vulnerabilities or threats are discovered.

1.7 Change Request Procedure

1.7.1 A written request for a configuration change must come from an authorized individual. The request will include a description, the business reason, impact, a start and end date, and a rollback procedure.

1.7.2 The Office of Cash Management with the Office of Information Technology, or their designees, will review change requests and approve or deny the change in whole or in part.

1.7.3 Configuration changes will be tested in a non-production environment and reviewed prior to change being implemented into the production environment.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy

applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of The CIO.

Software Development Policy

I. POLICY STATEMENT

Any payment application software or web-based applications that transmit, process, or store credit card information developed for use by Auburn University entities or for use on the Auburn University network, must adhere (at a minimum) to standards set forth in the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 Development Environment

- **1.1.1** Any software development must take place on a separate development / test infrastructure. It is strictly prohibited to develop or change production software on production systems without following the approved "Change Control Policy"
- **1.1.2** Production data may not be used in any development without being sanitized and all identifying sensitive data removed.
- **1.1.3** Test data, (IDs, accounts, data, etc.) must be removed prior to system being put into production.
- **1.1.4** Development staff and production staff must maintain a strict separation of duties, or an appropriate compensating control must be documented and approved by Office of Information Technology and the Office of Cash Management.
- **1.1.5** Display of credit card information within an application should be masked in accordance with the PCI DSS. Only the first 6 digits and/or the last 4 may be displayed.
- **1.1.6** A separate code review by an impartial group or automated software product will be completed prior to software being placed in the production environment.
- **1.1.7** Web-facing applications shall be located behind a web application firewall.
- **1.1.8** Software developers must be trained in secure coding techniques (to include how to avoid common coding vulnerabilities, how sensitive data is handled in memory, how to protect against broken authentication and session management.) Strict adherence to industry "best practices" and secure coding practices need to be adhered to in all aspects of the development of applications. For a definition of best practices, refer to http://owasp.org, http://www.cert.org/secure-coding/

1.2 Development Lifecycle

- **1.2.1** All Web based applications will be scanned for vulnerabilities by OIT security staff, or by an external third party, on a regular basis or when significant changes have been made.
- **1.2.2** Critical or Severe vulnerabilities will be addressed immediately and systems re-scanned for complete remediation. Failure to remediate will result in server quarantine.
- **1.2.3** When applications are no longer needed, they must be securely removed and all data destroyed or rendered unreadable. Backups of the system and development software should also be securely deleted / removed in compliance with the PCI Data Retention and Disposal Policy.
- **1.2.4** System change control procedures must be implemented and logged.
- **1.2.5** A rollback procedure must be documented and approved prior to any system change.

III. EFFECTIVE DATE

October 15, 2012
Updated: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Data Retention and Disposal Policy

I. POLICY STATEMENT

Card holder data storage must be approved by the Office of Cash Management and may only be stored according to provisions set forth in the Payment Card Industry Data Security Standards (PCI DSS.) When no longer needed for card processing requirements, stored card holder data must be removed from the Auburn University Card Holder Data Environment in a manner compliant with the standards set forth in the PCI DSS.

II. POLICY PRINCIPLES

1.1 Storage

1.1.1 The following credit card information is permitted to be stored only if there is an approved and documented business need. An Office of Cash Management approved written justification must be provided documenting the business need for retention. All data must be protected as described in all sections of the PCI DSS. The following card holder data, protected as required by the PCI DSS and approved by the Office of Cash Management, is permitted to be stored under this provision:

- **1.1.1.1** Primary Account Number (PAN)
- **1.1.1.2** Cardholder name
- **1.1.1.3** Service Code
- **1.1.1.4** Expiration Date

1.1.2 The following card holder data is not permitted to be stored: (exception to this is in "pre-authorization" see 1.1.3

- **1.1.2.1** Full Magnetic Stripe (Track 1 or 2 data)
- **1.1.2.2** CVV2, CVC2, CID, CAV2
- **1.1.2.3** PIN / PIN Block

1.1.3 Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction.

1.1.4 System and audit logs showing access to stored data must be retained for at least 1-year. Logs must be kept online and available for 90 days.

1.2 Disposal

1.3 All sensitive and credit card data must be destroyed when it is no longer required by legal, contractual, or business need.

1.3.1 Techniques for disposal of data on media is as follows:

- **1.3.1.1** Hard disks: must be overwritten as prescribed by the Auburn University Electronic Data Disposal Policy or physically destroyed.
- **1.3.1.2** Floppy disks: must be shredded.
- **1.3.1.3** Optical media (CD's, DVD's, Blue Ray, etc.) must be shredded
- **1.3.1.4** Other magnetic media, (USB Drives, storage cards, etc.) must be overwritten by an approved method, or as

Prescribed by the Auburn University Electronic Data Disposal Policy or otherwise destroyed.

1.3.1.5 Paper: must be cross-cut shredded, pulped or incinerated

1.3.2 Paper containing cardholder data, awaiting destruction, must be stored in a secure containers secured with a lock to prevent access to its contents.

1.3.3 Quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements must be in place.

III. EFFECTIVE DATE

August 30, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
Logging Controls Policy

I. POLICY STATEMENT

Actions that occur within the Auburn University Card Holder Data Environment must be logged in a manner compliant (at a minimum) with the standards set forth in the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

Logging is to be recorded to the level of detail to assist in the reconstruction of any event that takes place in the CDE. Therefore, a secure environment for log acquisition and storage is to be in place.

1.1 Events to be logged

- **1.1.1** Events shall be logged with the ability to associate recorded events to individual users. Logs shall contain enough information to reconstruct the following activities
  - **1.1.1.1** User access to any cardholder data
  - **1.1.1.2** Administrative access to any system that contains cardholder data and specific access of data
  - **1.1.1.3** All authentication attempts, (pass and/or fail)
  - **1.1.1.4** Creation or deletion of system level objects
  - **1.1.1.5** Configuration changes
  - **1.1.1.6** Modifications to any user accounts, including, but not limited to, creation, modification or escalation of privileges
  - **1.1.1.7** Access and changes to root or kernel system files
  - **1.1.1.8** Access and changes to log files including stopping or pausing of the logs.
- **1.1.2** Additionally, logs must contain the following fields:
  - **1.1.2.1** Date & Time
  - **1.1.2.2** Type of event
  - **1.1.2.3** Origination
  - **1.1.2.4** Identity of affected data, system or resource

1.2 Storage

Logs must not be stored on the same system from which they originate (authentication of users on a domain controller for example). Logs must be written to a separate robust system that has its own specific security parameters on the internal LAN.

- **1.2.1** Limit access to logs to approved authorized personnel.
- **1.2.2** Logs records must have time and date stamps
- **1.2.3** File integrity monitoring software shall be installed to monitor all access and changes to log files.
- **1.2.4** Logs shall be retained for at least 1 year with at least 3 months available immediately.
- **1.2.5** Audits must be conducted to verify the viability of logs
- **1.2.6** Logs must be reviewed daily. It is permitted to incorporate software for this purpose. The appropriate triggers and alerts must be tested regularly.
- **1.2.7** A documented procedure shall be in place to respond to any alerts generated by log review or file integrity monitoring.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants and system administrators to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
Backup Control Policy

I. POLICY STATEMENT

Backup subsystems serving the Auburn University Card Holder Data Environment must be implemented in a manner in compliance (at a minimum) with the standards set forth in the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1. Storage

The backup subsystem must be identified as part of the CDE. Cardholder data on the subsystem must be rendered unreadable and unable to be re-constructed through un-approved means. Backups of sensitive data must be completed on a regular basis. Data should be checked regularly for restoration applicability.

1.1.1. Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden.

1.1.2. System and audit logs showing access to CDE data must be retained for at least 1-year. The previous 90 days must be kept available and online.

1.2. Control

1.2.1. All media with sensitive data must be marked as confidential and strict control must be maintained in storage and accessibility of the media.

1.2.2. Media must be stored in a secure location approved by management. This location must have limited accessibility to only those that need access. All access to the location must be logged. Security of facility must be reviewed annually.

1.2.3. All media couriers and transport mechanisms must be certified by the Office of Cash Management.

1.2.4. Any media sent outside the CDE must be positively logged in and out. A record must be maintained of all media in storage and use as well as its whereabouts.

1.3. Disposal

1.3.1. All media that is no longer needed, or has reached end-of-life, must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques for magnetic media is detailed in the Auburn University Data Retention and Disposal Policy. Further guidance on destruction can be found in the Cardholder Data Environment: Data Retention and Disposal Policy.

III. EFFECTIVE DATE

October 15, 2012 Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGEMENT

Responsible Office: Office of Cash Management and Office of the CIO
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list.

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy id subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
Service Provider Policy

I. POLICY STATEMENT

Third parties, with whom Auburn University cardholder data is shared, must be contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the cardholder data which they have been/will be entrusted with. Any agreements with third parties, with whom cardholder data is/will be shared, must be approved by the Office of Cash Management. Only the minimum amount of data needed to complete the transaction will be shared with third parties. All interaction must be documented and logged.

II. POLICY PRINCIPLES

Contracts with third-party providers must delineate each party's roles and responsibilities with respect to PCI-DSS compliance. The following language, provided as a **SAMPLE**, illustrates the type of language that might be included a contract addendum with a third-party service provider who processes, transmits, stores or controls the payment path for cardholder data on behalf of Auburn University, if the existing contract does not address the matter sufficiently. (The Office of Payment and Procurement Services must be consulted prior to issuance of any contract.)

Whereas *Auburn University (AUBURN) secures services from _____ ("Vendor") under a Contract dated_____(date), which services involve the processing of merchant card transactions, specifically_____; and*

Whereas *AUBURN is required to adhere to the Payment Card Industry Data Security Standard (PCI DSS) promulgated by the PCI Security Standards Council; and*

Whereas *Vendor processes, transmits, stores and/or controls the payment path for cardholder data in the performance of services provided to AUBURN, and is therefore considered a "service provider" under Requirement 12.8 of the PCI DSS; and*

Whereas *Requirement 12.8.2 of the PCI DSS requires AUBURN to maintain a written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data that the service provider possesses; and*

Whereas *Requirement 12.8.4 of the PCI DSS requires AUBURN to maintain a program to monitor the service provider's PCI DSS compliance status;*

and Whereas *Requirement 12.8.5 of the PCI DSS requires each party to this agreement to acknowledge which PCI DSS requirements they will be responsible for;*

It is hereby agreed that:

1) *Vendor agrees that it is responsible for the security of cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data. Vendor will notify AUBURN within twenty-four hours if it has knowledge of, or can reasonably expect that, a security breach has occurred. Vendor takes responsibility for the payment of fines, penalties, lawsuits and other costs*

incurred by AUBURN that result from a breach that can be traced to the action or inaction of the VENDOR and will assume 100% of those costs assuming no contributory negligence on the part of AUBURN, merchant acquirer, merchant bank, or other negligent third party.

2) *Vendor affirms that, as of the effective date of this Addendum, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS including undergoing a Level 2, or Level 1, PCI audit as necessary.*

3) *Vendor agrees to supply the current status of Vendor's PCI DSS compliance and evidence of its most recent validation of compliance upon execution of this addendum to AUBURN. Vendor must supply to AUBURN a new status report and evidence of validation of compliance at least annually throughout the duration of this contract.*

4) *Vendor will immediately notify AUBURN if it learns that it, or one of its service providers, is no longer PCI DSS compliant and will immediately provide AUBURN the steps being taken to remediate the non-compliance status. In no event should Vendor's notification to AUBURN be later than seven (7) calendar days after Vendor learns it is no longer PCI DSS complaint. Should Vendor fail to become PCI DSS compliant with a timeframe deemed reasonable by AUBURN, AUBURN shall, at its discretion terminate this Vendor's services.*

5) *Vendor acknowledges that any indemnification provided for under the referenced Contract applies to the failure of the Vendor to be and to remain PCI DSS compliant*.

6) Vendor shall be responsible for all PCI DSS requirements for logging and monitoring of equipment and applications located on the vendor's premises, private networks extended onto AUBURN's campus, as well as maintenance of devices and applications for which VENDOR maintains administrative control. Vendor shall be responsible for all physical security of devices located on the vendor's premises. Vendor shall complete necessary PCI DSS vulnerability scans and penetration tests on devices on its networks or private networks extended onto AUBURN's campus.

7) AUBURN shall be responsible for all PCI DSS requirements for logging, monitoring of equipment and applications located on the AUBURN's campus for which it has administrative control. AUBURN shall be responsible for all physical security of devices located on the AUBURN's premises. AUBURN shall complete necessary PCI DSS vulnerability scans and penetration tests on devices on its network.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: June 18, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGEMENT

Responsible Office: Office of Cash Management and Office of the CIO
Responsible Executive: Executive VP for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment Wireless Usage Policy

I. POLICY STATEMENT

Approval from the Office of Cash Management and the CIO must be obtained and documented prior to using any wireless technology to store, process, or transmit cardholder data. All such use must (at a minimum) adhere to provisions of the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 Communications must utilize industry-standard best practices to implement strong encryption for authentication and transmission

1.2 Strong encryption keys must be used for wireless communication. Encryption must follow the same process as those described in the PCI-DSS Encryption Policy.

1.3 Appropriate network segmentation must be maintained in the CDE. Any wireless network used for transmission of cardholder data must have a perimeter firewall installed at the ingress and egress point of the wireless network environment.

1.4 Use of general faculty, staff, and student accessible WiFi networks to transmit cardholder data is strictly prohibited.

1.5 Scanning must be completed quarterly to verify that no un-authorized wireless networks have been installed in the CDE. If scanning is not feasible, a Wireless Intrusion Detection / Protection system may be used.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO
Responsible Executive: Executive V.P. for Business and Finance
Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment Encryption Policy

I. POLICY STATEMENT

All confidential and/or sensitive cardholder electronic data within the Auburn University Card Holder Data Environment must be protected (at a minimum) according to provisions set forth in the Payment Card Industry Data Security Standards.

II. POLICY PRINCIPLES

1.1 At a minimum, anytime the Primary Account Number is stored or transmitted electronically it must be protected according to the standards specified in this policy.

1.2 Encryption Keys

- **1.2.1** Only Strong encryption can be utilized to protect sensitive data. These methods are defined by the PCI DSS;
  - **1.2.1.1** 3DES
  - **1.2.1.2** AES
  - **1.2.1.3** Proprietary Vendor encryption providing it is approved in the PA-DSS
  - **1.2.1.4** TLS
  - **1.2.1.5** IPSEC
- **1.2.2** Encryption keys must be protected in the following manner;
  - **1.2.2.1** Have dual custodianship with the fewest number of custodians, such that at least two people are required to perform and key management operations and no one person has access to the authentication materials of another
  - **1.2.2.2** Clear text images of the keys must be kept locked in a tamper proof manner and in the fewest possible locations and forms.
  - **1.2.2.3** System and audit logs showing access to this data must be retained for at least 1-year. 90 days must be kept online and available for 90 days

1.3 Documentation

- **1.3.1** All process and procedures for the generation, use and destruction of cryptographic keys must be fully documented.
- **1.3.2** Require key custodians to acknowledge and accept responsibilities of their role as such by use of a formal signature.

1.4 Use

- **1.4.1** All protected data whether at rest or online, must be rendered unreadable using techniques such as encryption, truncation, 1-way hashing, tokenization, etc.
- **1.4.2** If disk encryption is used as opposed to table, column or file encryption, tables in databases holding sensitive information must be protected using techniques listed above (1.4.1) and logical access must be managed separately and independently of native operating system authentication and access control mechanisms

1.4.3 All data exchanged between systems and third parties must be done utilizing these strong encryption techniques.

1.4.4 Keys must be rotated at a minimum of 1 year intervals

1.5 Destruction

1.5.1 Old keys must be destroyed when no longer used, or confidence in the keys integrity may have become compromised.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment
Incident Reporting Policy

I. POLICY STATEMENT

All suspected incidents taking place within the Auburn University Card Holder Data Environment must be reported when discovered. Systems suspected of a breach must be preserved (at a minimum) according to provisions set forth in the Payment Card Industry Data Security Standards and the Auburn University Incident Response Policy.

II. POLICY PRINCIPLES

1.1 All merchants must familiarize themselves with the Auburn University Incident Response Policy and upon a suspected breach notify appropriate parties as stated therein.

1.2 When suspecting a breach, **only perform actions as directed** through consultation with the OIT information security group and the Office of Cash Management and **IMMEDIATELY** cease using the device and connected systems. OIT shall determine how best to isolate the affected systems from the network.

1.3 The card brands (MasterCard, Visa, Discover, American Express) will determine whether or not an independent forensics investigation will be initiated on the compromised device(s).

1.4 Affected systems should be physically secured (and remain connected to a power supply) to prevent unauthorized tampering.

1.5 Affected systems will not be brought back on-line until consultation and approval from the card brands, CIO and the Office of Cash Management.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 18, 2014, March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

XI. EXCLUSIONS

None.

XII. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the CIO.

Cardholder Data Environment
Security Awareness Policy

I. POLICY STATEMENT

Individuals with access to computers connected to the Cardholder Data Environment must annually complete a cyber-security awareness program, for which a record of attendance/completion will be centrally maintained. Individuals with access to computers connected to the CDE must acknowledge that they have read and understand all Payment Card Data Security Policies.

II. POLICY PRINCIPLES

Auburn University is committed to protecting cardholder. In light of this commitment, Auburn University will facilitate a centralized cyber-security awareness program to ensure employees with access to resources connected to the CDE possess a common framework and content knowledge regarding the protection of these information assets.

III. EFFECTIVE DATE

October 15, 2012
Revised: March 1, 2015

IV. APPLICABILITY

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to Auburn University's CDE, including all personnel affiliated with third parties. This policy applies to all equipment connected to the Auburn University CDE network.

V. POLICY MANAGMENT

Responsible Office: Office of Cash Management and Office of the CIO

Responsible Executive: Executive V.P. for Business and Finance

Responsible Officer: CIO & Director of Cash Management

VI. DEFINITIONS

See attached definition list

VII. POLICY PROCEDURES

Individual merchants to develop and document relevant procedures.

VIII. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Office of Cash Management and the Office of the CIO.

Cardholder Data Environment Definitions

Access Control	Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.
Account Data	Account data consists of cardholder data plus sensitive authentication data. See Cardholder Data and Sensitive Authentication Data.
Acquirer	Also referred to as "acquiring bank" or "acquiring financial institution." Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Adware	Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.
AES	Abbreviation for "Advanced Encryption Standard." Block cipher used in symmetric key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or "FIPS 197"). See Strong Cryptography.
ANSI	Acronym for "American National Standards Institute." Private, non- profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
Anti-Virus	Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.
Application	Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.
Approved Scanning Vendor (ASV)	Company approved by the PCI SSC to conduct external vulnerability scanning services.
Auburn University Cardholder Data Environment (AU CDE)	For purposes of these policies, Auburn University refers to AU Main Campus, Auburn University at Montgomery, the Alabama Cooperative Extension System, the Alabama Agricultural Experiment Stations and all affiliated organizations. (See Cardholder Data Environment.)
Audit Log	Also referred to as an "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Audit Trail	See Audit Log
Authentication	Process of verifying identity of an individual, device, or process.

	Authentication typically occurs through the use of one or more authentication factors such as: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric
Authentication Credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process
Authorization	Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
Brute Force	Brute force is a trial and error method used to decode encrypted data or guess a password through exhaustive effort.
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: • CAV – Card Authentication Value (JCB payment cards) • CVC – Card Validation Code (MasterCard payment cards) • CVV – Card Verification Value (Visa and Discover payment cards) • CSC – Card Security Code (American Express) (2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four- digit non-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: • CID – Card Identification Number (American Express and Discover payment cards) • CAV2 – Card Authentication Value 2 (JCB payment cards) • CVC2 – Card Validation Code 2 (MasterCard payment cards) • CVV2 – Card Verification Value 2 (Visa payment cards)

Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
Cardholder Data Environment (CDE)	The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.
CERT	Acronym for Carnegie Mellon University's "Computer Emergency Response Team." The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.
CIS	Acronym for "Center for Internet Security." Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.
Column-Level Database Encryption	Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see Disk Encryption or File-Level Encryption.
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: (1)) Meet the intent and rigor of the original PCI DSS requirement; (2) Provide a similar level of defense as the original PCI DSS requirement; (3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. See "Compensating Controls" Appendices B and C in PCI DSS Requirements and Security Assessment Procedures for guidance on the use of compensating controls.

Compromise	Also referred to as “data compromise,” or “data breach.” Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Console	Screen and keyboard which permits access and control of a server, mainframe computer or other system type in a networked environment.
Consumer	Individual purchasing goods, services, or both.
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.
Cryptoperiod	The time span during which a specific cryptographic key can be used for its defined purpose based on, for example, a defined period of time and/or the amount of cipher-text that has been produced, and according to industry best practices and guidelines (for example, NIST Special Publication 800-57).
Database	Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.
Database Administrator	Also referred to as “DBA.” Individual responsible for managing and administering databases.
Default Accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Degaussing	Also called “disk degaussing.” Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.

Disk Encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, File- Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub- network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
DNS	Acronym for "Domain Name System" or "domain name server." System that stores information associated with domain names in a distributed database on networks such as the Internet.
DSS	Acronym for "Data Security Standard" and also referred to as "PCI DSS."
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge.)
Dynamic Packet Filtering	See Stateful Inspection
ECC	Acronym for "Elliptic Curve Cryptography." Approach to public-key cryptography based on elliptic curves over finite fields. See Strong Cryptography.
Egress Filtering	Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the network.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See Strong Cryptography.

Encryption Algorithm	A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again. See Strong Cryptography.
Entity	Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.
File Integrity Monitoring	Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see Disk Encryption or Column-Level Database Encryption.
FIPS	Acronym for "Federal Information Processing Standards." Standards that are publicly recognized by the U.S. Federal Government; also for use by non- government agencies and contractors.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology.
GPRS	Acronym for "General Packet Radio Service." Mobile data service available to users of GSM mobile phones. Recognized for efficient use of limited bandwidth. Particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing.
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via Strong Cryptography. Hashing is a (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). A hash function should have the following properties:

	(1) It is computationally infeasible to determine the original input given only the hash code, (2) It is computationally infeasible to find two inputs that give the same hash code. In the context of PCI DSS, hashing must be applied to the entire PAN for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data includes a salt value as input to the hashing function (see Salt).
Host	Main computer hardware on which computer software is resident.
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.
HTTP	Acronym for "hypertext transfer protocol." Open internet protocol to transfer or convey information on the World Wide Web.
HTTPS	Acronym for "hypertext transfer protocol over secure socket layer." Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security- sensitive communication such as web-based logins.
Hypervisor	Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM).
ID	Identifier for a particular user or application.
IDS	Acronym for "intrusion detection system." Software or hardware used to identify and alert on network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected.
IETF	Acronym for "Internet Engineering Task Force." Large, open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of Internet. The IETF has no formal membership and is open to any interested individual.

Index Token	A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information Security	Protection of information to insure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Ingress Filtering	Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network.
Insecure Protocol/Service/Port	A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that transmit data and authentication credentials (e.g., password/passphrase in clear-text over the Internet), or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer on the Internet.
IP Address Spoofing	Attack technique used by a malicious individual to gain unauthorized access to computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.
IPS	Acronym for "intrusion prevention system." Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.
IPSEC	Abbreviation for "Internet Protocol Security." Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer.
ISO	Better known as "International Organization for Standardization." Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland, that coordinates the system.
Issuer	Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as "issuing bank" or "issuing financial institution".

Issuing Service	Examples of issuing services may include but are not limited to authorization and card personalization.
Key	In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to ciphertext. The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message. See Strong Cryptography.
Key Management	In cryptography, it is the set of processes and mechanisms which support key establishment and maintenance, including replacing older keys with new keys as necessary.
LAN	Acronym for "local area network." A group of computer and/or other devices that share a common communications line, often in a building or group of buildings.
LDAP	Acronym for "Lightweight Directory Access Protocol." Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected resources.
Least Privilege	The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
Log	See Audit Log.
LPAR	Abbreviation for "logical partition." A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces.
MAC	Acronym for "message authentication code." In cryptography, it is a small piece of information used to authenticate a message. See Strong Cryptography.
MAC Address	Abbreviation for "media access control address." Unique identifying value assigned by manufacturers to network adapters and network interface cards.
Magnetic-Stripe Data	Also referred to as "track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

Mainframe	Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.
Malicious Software / Malware	Software designed to infiltrate or damage a computer system without the owner's knowledge or consent. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
Monitoring	Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
MPLS	Acronym for “multi protocol label switching.” Network or telecommunications mechanism designed for connecting a group of packet-switched networks.
NAT	Acronym for “network address translation.” Known as network masquerading or IP masquerading. Change of an IP address used within one network to a different IP address known within another network.
Network	Two or more computers connected together via physical or wireless means.
Network Administrator	Personnel responsible for managing the network within an entity. Responsibilities typically include but are not limited to network security, installations, upgrades, maintenance and activity monitoring.
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Network Security Scan	Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.
Network Segmentation	Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement. See System Components.
NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration. Their mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life.
NMAP	Security-scanning software that maps networks and identifies open ports in network resources.
Non-Computer Users	Individuals, excluding cardholders, who access system components, including but not limited to employees, administrators, and third parties.
NTP	Acronym for "Network Time Protocol." Protocol for synchronizing the clocks of computer systems, network devices and other system components.
Off-the-Shelf	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Operating System / OS	Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.
OWASP	Acronym for "Open Web Application Security Project." A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (See http://www.owasp.org).
Pad	In cryptography, the one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain- text and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable.

Off-the-Shelf	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Operating System / OS	Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.
OWASP	Acronym for "Open Web Application Security Project." A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (See http://www.owasp.org).
Pad	In cryptography, the one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain- text and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable.
PA-QSA	Acronym for "Payment Application Qualified Security Assessor," company approved by the PCI SSC to conduct assessments on payment applications against the PA-DSS.
Parameterized Queries	A means of structuring SQL queries to limit escaping and thus prevent injection attacks.
Password / Passphrase	A string of characters that serve as an authenticator of the user.
PAT	Acronym for "port address translation" and also referred to as "network address port translation." Type of NAT that also translates the port numbers
Patch	Update to existing software to add functionality or to correct a defect.
Payment Application	Any application that stores, processes, or transmits cardholder data as part of authorization or settlement
Payment Card Industry Data Security Standards (PCI-DSS)	PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data. It presents common-sense steps that mirror best security practices. For more information see (http://www.pcisecuritystandards.org)
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

PCI	Acronym for “Payment Card Industry.”
PDA	Acronym for “personal data assistant” or “personal digital assistant.” Handheld mobile devices with capabilities such as mobile phones, e-mail, or web browser.
PED	PIN entry device
Penetration Test	Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.
Personal Identification Number (PIN)	Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.
Personally Identifiable Information	Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.
Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.
POI	Acronym for “Point of Interaction,” the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic- stripe card-based payment transactions.
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures

POS	Acronym for “point of sale.” Hardware and/or software used to process payment card transactions at merchant locations.
Primary Account Number (PAN)	Also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Private Network	Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers.
Procedure	Descriptive narrative for a policy. Procedure is the “how to” for a policy and describes how the policy is to be implemented.
Protocol	Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.
PTS	Acronym for “PIN Transaction Security,” PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org.
Public Network	Network established and operated by a telecommunications provider or the University, for specific purpose of providing data transmission services for the public or the University community as a whole (as opposed to a Private Network with restricted access).
PVV	Acronym for “PIN verification value.” Discretionary value encoded in magnetic stripe of payment card.
QSA	Acronym for “Qualified Security Assessor,” company approved by the PCI SSC to conduct PCI DSS on-site assessments.
Quarantine	At times it becomes necessary to isolate a computer from the campus and or CDE network in order to protect the integrity of the network and/or the institution. The network quarantine prevents network traffic from getting into or out of the computer.
RADIUS	Abbreviation for “Remote Authentication Dial-In User Service.” Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication.

Re-keying	Process of changing cryptographic keys. Periodic re-keying limits the amount of data encrypted by a single key.
Remote Access	Access to computer networks form a remote location, typically originating from outside the network. An example of technology for remote access is VPN.
Remote Lab Environment	A lab that is not maintained by the PA-QSA.
Removable Electronic Media	Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD- ROM, USB flash drives and removable hard drives.
Report on Compliance	Also referred to as "ROC." Report containing details documenting an entity's compliance status with the PCI DDS.
Report on Validation	Also referred to as "ROV." Report containing details documenting a payment application's compliance with the PCI PA-DDS.
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
RFC 1918	The standard identified by the Internet Engineering Task Force (IETF) that defines the usage and appropriate address ranges for private (non-internet routable) networks.
Risk Analysis/Risk Assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
Role Based Access Control	Control used to restrict access by specific authorized users based on their job responsibilities.
Rootkit	Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.

Salt	Random string that is concatenated with other data prior to being operated on by a hash function. See also Hash.
Sampling	The process of selecting a cross-section of a group that is representative of the entire group. Sampling may be used by assessors to reduce overall testing efforts, when it is validated that an entity has standard, centralized PCI DSS security and operational processes and controls in place. Sampling is not a PCI DSS requirement.
SANS	Acronym for "SysAdmin, Audit, Networking and Security," an institute that provides computer security training and professional certification. (See www.sans.org.)
SAQ	Acronym for "Self-Assessment Questionnaire." Tool used by any entity to validate its own compliance with the PCI DSS.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.
SDLC	Acronym for "system development life cycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation.
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.
Secure Wipe	Also called "secure delete," a program utility used to delete specific files permanently from a computer system.
Security Officer	Primary responsible person for an entity's security-related affairs.
Security Policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information
Security Protocols	Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to TLS, IPSEC, SSH, etc.
Sensitive Area	Any data center, server room or any area that houses systems that stores, processes, or transmits cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Separation of Duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.
Server	Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.
SHA-1/SHA-2	Acronym for "Secure Hash Algorithm." A family or set of related cryptographic hash functions including SHA-1 and SHA-2. See Strong Cryptography.
Smart Card	Also referred to as "chip card" or "IC card (integrated circuit card)." A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the "chip," contain payment card data including but not limited to data equivalent to the magnetic-stripe data.
SNMP	Acronym for "Simple Network Management Protocol." Supports monitoring of network attached devices for any conditions that warrant administrative attention.
Split Knowledge	Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
Spyware	Type of malicious software that when installed, intercepts or takes partial control of the user's computer without the user's consent.
SQL	Acronym for "Structured Query Language." Computer language used to create, modify, and retrieve data from relational database management systems.
SQL Injection	Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.

SSH	Abbreviation for “Secure Shell.” Protocol suite providing encryption for network services like remote login or remote file transfer.
SSL	Acronym for “Secure Sockets Layer.” No longer considered Strong Cryptography under PCI DSS. Use TLS instead.
Stateful Inspection	Also called “dynamic packet filtering,” it is a firewall capability that provides enhanced security by keeping track of communications packets. Only incoming packets with a proper response (“established connections”) are allowed through the firewall.
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or “one way”). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (http://csrc.nist.gov/publications/) for more information.
SysAdmin	Abbreviation for “system administrator.” Individual with elevated privileges who is responsible for managing a computer system or network.
System Components	Any network component, server, or application included in or connected to the cardholder data environment.
System-level object	Anything on a system component that is required for its operation, including but not limited to application executable and configuration files, system configuration files, static and shared libraries & DLL's, system executables, device drivers and device configuration files, and added third-party components.
TACACS	Acronym for “Terminal Access Controller Access Control System.” Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication.

TCP	Acronym for "Transmission Control Protocol." Basic communication language or protocol of the Internet.
TDES	Acronym for "Triple Data Encryption Standard" and also known as "3DES" or "Triple DES." Block cipher formed from the DES cipher by using it three times. See Strong Cryptography.
TELNET	Abbreviation for "telephone network protocol." Typically used to provide user- oriented command line login sessions to devices on a network. User credentials are transmitted in clear text.
Threat Condition	ThreatCondition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization
TLS	Acronym for "Transport Layer Security." Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Token	A value provided by hardware or software that usually works with an authentication server or VPN to perform dynamic or two-factor authentication. See RADIUS, TACACS, and VPN.
Transaction Data	Data related to electronic payment card transaction.
Trojan	Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.
Truncation	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See Masking for protection of PAN when displayed on screens, paper receipts, etc.
Trusted Network	Network of an organization that is within the organization's ability to control or manage all activity.
Two-Factor Authentication	Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

Untrusted Network	Network that is external to the networks belonging to an organization and/or which is out of the organization's ability to control or manage all activity.
User Accounts	An established relationship between a user and a computer, network or information service. User accounts are assigned a username
Virtual Appliance (VA)	A VA takes the concept of a pre-configured device for performing a specific set of functions and run this device as a workload. Often, an existing network device is virtualized to run as a virtual appliance, such as a router, switch, or firewall.
Virtual Hypervisor	See Hypervisor.
Virtual Machine	A self-contained operating environment that behaves like a separate computer. It is also known as the "Guest," and runs on top of a hypervisor.
Virtual Machine Monitor (VMM)	The VMM is included with the hypervisor and is software that implements virtual machine hardware abstraction. It manages the system's processor, memory, and other resources to allocate what each guest operating system requires.
Virtual Private Network (VPN)	A computer network in which some of the connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.
Virtual Switch or Router	A virtual switch or router is a logical entity that presents network infrastructure level data routing and switching functionality. A virtual switch is an integral part of a virtualized server platform such as a hypervisor driver, module, or plug-in.
Virtual Terminal	A virtual terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

Virtualization	Virtualization refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage.
VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network.
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
WAN	Acronym for "wide area network." Computer network covering a large area, often a regional or company-wide computer system.
Web Application	An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.
Web Server	Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).
WEP	Acronym for "Wired Equivalent Privacy." Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes. See WPA.
Wireless Access Point	Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.
Wireless Networks	Network that connects computers without a physical connection to wires.
WLAN	Acronym for "wireless local area network." Local area network that links two or more computers or devices without wires.
WPA/WPA2	Acronym for "WiFi Protected Access." Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA