CALIFORNIA STATE UNIVERSITY
FULLERTON

PCI DSS INFORMATION SECURITY STANDARDS

August 5, 2021

TABLE OF CONTENTS

CALIFORNIA STATE UNIVERSITY
FULLERTON

PCI DSS INFORMATION SECURITY STANDARDS

August 5, 2021

I. OVERVIEW

The Board of Trustees of the California State University (CSU) is responsible for protecting the confidentiality, integrity and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

It is the collective responsibility of all users to ensure:

a. Confidentiality of information which the CSU must protect from unauthorized access.
b. Integrity and availability of information stored on or processed by CSU information systems.
c. Compliance with applicable laws, regulations, and C SU/campus policies governing information security and privacy protection.

The CSU Information Security Policy and Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the CSU's core mission and campus academic and administrative goals.

CSU Information Security Policy applies to California State University, Fullerton including the following:

a. Central and departmentally-managed campus information assets
b. All campus employed users or any other person with access to campus information assets
c. All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic)
d. Information technology facilities, applications, hardware systems, and network resources owned or managed by the C SU
e. Auxiliaries, external businesses and organizations that utilize campus information assets

The purpose of the CSUF Information Security Standard is to provide guidelines within CSU Policy specifically in compliance with PCI DSS Requirements, protecting the security and integrity of cardholder data

II. DEFINITIONS, IMPLEMENTATION & ACCOUNTABILITY

(Requirement 1.1.5 & Requirement 7)See IT Organization Chart IT_Senior_Leadership_Team_Org_Chart.pdf (fullerton.edu), *President's Directive #13*

A. The **University Chief Information Security Officer; CITO**; is the campus Chief Information Technology Officer who has been designated by the President to oversee Information Security policy and the coordination of information security efforts across the university. Working with CSUF senior management the CITO coordinates the process to build a university-wide

information security strategy and vision. The CITO is charged with the responsibility for building an information security-conscious culture and infrastructure for CSUF.

B. The **University Information Security Officer; ISO**; is an appropriate administrator designated by the President and delegated responsibility by the CITO for the security of all protected information collected, used, maintained, or released by the University as well as leads the development of a campus wide information security strategy.

   The Information Security Officer directly reports to the University's Chief Information/Technology Officer and is a member of the Information Technology Leadership Team. The ISO works in collaboration with other managers in Information Technology and administrators from other divisions to establish an effective information security program and support the University mission

   The Information Security Officer recommends and develops information security solutions to provide detection, prevention, containment, and deterrence mechanisms to protect and maintain the integrity of the campus data infrastructure, systems, applications and physical assets.

C. **Custodians of Records** are defined as appropriate administrators in charge of offices or departments with functional ownership of protected information (e.g., the Director of Admissions & Records, the Director of Financial Aid, the Director of the Student Health Center, University Controller and the Executive Director of Human Resources). Custodians of Records are responsible for securing protected information under the control of their respective department or area of responsibility, including electronic databases, printed reports, and submitted materials.

D. **Appropriate Administrators** are supervisors or managers included in the Management Personnel Plan. Appropriate administrators are responsible for applying federal and state laws and CSU and policies and procedures regarding protected information, and for granting, monitoring, and managing access to protected information by employees or contractors reporting to them.

E. **Protected Information** includes information identifying or describing an individual. Different language is used in various federal and state regulations and CSU policies to describe protected information. Level Protected information based on CSU Data Classification Standard

Failure to comply with applicable federal and state laws and regulations, including but not limited to PCI requirements as defined by PCI DSS Councils may result in fines, penalties, exclusion from government funded programs, discipline, litigation, adverse publicity, and an array of other impacts that could impede the mission of the University.

III. REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

This guidance is intended for the university to understand scoping and segmentation principles when applying PCI DSS to current environment. The campus must evaluate which system components should be covered by PCI DSS requirements. Segmentation method for purposes of reducing PCI DSS scope include firewalls and router configurations to prevent traffic passing between out-of-scope networks and the CDE, network configurations that prevent communications between different systems and/or subnets, and physical access controls

This policy creates standards for Firewall Policies/Rules and Procedures to ensure institutional data security and best practices while providing service and support to the University's academic and business community.

Additionally, this policy is intended to create a process for annual review and assessment of in-scope inventory and existing Firewall Policies/Rules.

The policy also stipulates the process and requirements for the creation of new Firewall Policies/Rules.

A. BOUNDARY PROTECTION AND ISOLATION

(ICSUAM 8045.S301 & 8050.S100)

Division of Information Technology requires the following:

1. Access to campus networks must be controlled by a technical solution, which permits only authorized inbound traffic. It must be determined, based on risk analysis, the extent to which outbound traffic is blocked or limited.
2. Appropriately separate network access to public information system resources from those which store protected Level 1 and Level 2 information.
3. Establish zoning or separation within internal networks based on established trust relationships, authorized services, and data classification in order to ensure that protected information is not made available to unauthorized persons.
4. All unnecessary services (e.g., Web service, SNMP) on any system which is directly accessible from the internet must be disabled.
5. All privileged administrator network access to systems which are directly accessible from the internet must be encrypted and multi-factor authenticated.
6. Maintain documentation as follows:
    a. A formal, documented process for approving and testing configuration changes to its network and network control devices.
    b. Formal network configuration document that defines all open ports and services on systems directly accessible from the internet.

c. Justification and risk analysis as appropriate for any allowed service or protocol.
d. Annual review for all configurations and firewall rules associated with border devices and/or systems directly accessible from the Internet to determine if the rule is still valid, still necessary and performing the function for which it was requested.

B. SCOPING CONCEPTS

Systems located within the CDE are in scope, irrespective of their functionality or the reason why they are in the CDE.

Similarly, systems that connect to a system in the CDE are in scope, irrespective of their functionality or the reason they have connectivity to the CDE.

The diagram in Appendix A illustrate how system components can be categorized using several factors:

a) Whether account data (CHD/SAD) is being stored, processed, or transmitted.
b) The connectivity between the system component and the CDE.
c) Whether a system component impacts the security of the CDE.

Information Technology maintains an inventory identifying Level 1 protected data. Normally, responsibility for Level 1 protected data resides with the manager of the campus program that employs the information. When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

a) Which program collected the information?
b) Which program is responsible for the accuracy and integrity of the information?
c) Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.
d) Which program has the most knowledge of the useful value of the information?
e) Which program would be most affected, and to what degree, if the information were lost, inaccurate, compromised, delayed, or disclosed to unauthorized parties.

The university must keep inventory of all in-scope system components within the Cardholder Data Environment (CDE) network zone *(see ICSUAM 8050.S100 section 1.2 Inventory)*. Financial Services department in Administration & Finance maintains a list of PCI In-scope system components. PCICC shall review and update the list, annually.

PCICC ensures that all In-scope system components are properly segmented.

C. ACCESS TO CDE

Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access management and other non-console administrative access.

D. RULES ON PCI FIREWALL AND ROUTER

1. The only connections permitted into and out of the CDE are to Shared Services, via specifically designated ports and systems, and only where there is a documented business need.
2. All connection attempts between the University LAN and the CDE are actively blocked (no traffic that originated in the University LAN is allowed into the CDE).
3. Communications between Shared Services and the University LAN:
    a. Are permitted only between designated systems, ports, services etc., and all other connection attempts are blocked.
    b. Are limited by business need, however, no email allowed—for example, connectivity between workstations and Active Directory Server is limited to only network authentication traffic.
4. Communication between CDE are also actively blocked
5. No CHD is stored, processed, or transmitted outside the CDE network except via secured network connections to the acquiring bank/processor (i.e., eMarket, Storefront, 3rd Party Gateways, or P2PE solutions,).
6. All applicable PCI DSS requirements are applied:
    a. To the CDE and Shared Services networks and system components
    b. To manage and secure connectivity between the CDE and Shared Services, including firewalls, ACLs, IDS/IPS, anti-malware and other threat defense tools and techniques
    c. To manage and secure inbound/outbound traffic between Shared Services and the University LAN.
7. Physical access to the CDE and Shared Services network is restricted to Division of Information Technology/Infrastructure Services personnel, as defined by business need.
8. All network switches, router and hubs to be install within CDE must be authorized by Information Technology Network & Security Team
9. Information Technology prohibits use unauthorized network switches and hubs.
10. Install perimeter firewalls between all wireless networks and cardholder data environment, and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), deny all traffic from the wireless environment into and the cardholder data environment.
11. Network & Security Team actively monitors & inspects traffic and activity between Shared Services and the CDE, and within the CDE, on a daily basis, to detect anomalies and reduce the risk of a Shared Services compromise leading to a compromise of the CDE.
12. *Third Party Service Provider (i.e. SecureWorks) reviews daily, CDE data logs and notify Information Technology Team of any network anomalies in CDE environment.*

"Shared services" are common system components that provide services, such as authentication or management support, to system components across the university enterprise, including to both CDE systems and out-of-scope systems

Common shared services include, but are not limited to:

1. Directory and authentication (e.g., Active Directory, LDAP/ AAA)
2. NTP – Network Time Protocol
3. DNS – Domain Name Service
4. DHCP – Dynamic Host Configuration Protocol
5. SMTP – Simple Mail Transfer Protocol
6. Monitoring and scanning tools
7. Backup tools
8. Anti-virus and patch deployment servers
9. CDE Log server

Other than high-level network diagram, a separate PCI CDE diagram is maintained and review, annually.

E. FIREWALL PRACTICE & APPLICATION

The Practice/Standard applies to all existing firewalls and new firewalls introduced to the California State University, Fullerton (CSUF) network and computing infrastructure. This includes all network firewalls and server/systems firewalls specific to enterprise applications and databases.

F. PRACTICE/STANDARD

Requests for Firewall Policies/Rules must be made using the IT Help Desk ticketing system (Service-Now). Additionally, all Firewall Policies/Rules when created, modified or disabled requires a CHANGE MANAGEMENT APPROVAL (see IT Change Management Process). The approval shall be included within the comment field, time of entry, the date of entry, purpose of the policy/rule, and initials of person making the entry.

Requested Policies/Rules must contain information that includes but not limited to the following:

1. Rationale for needing the policy
2. system name,
3. application,
4. object or group name(s),
5. list of the responsible party or organization,
6. system IP address
7. port(s) required prior to requesting any virtual or physical server implementation.

For security and audit purposes, Firewall Policies/Rules shall be reviewed every 6 months or whenever an existing Policy/Rule, Object, or Groups Category is modified or disabled. Our practice also requires

that IT Network Administrators complete/update the Comment Filed whenever any entry is made or changed in the firewall. The IT Network Team will complete periodic review work and, if funding permits, a third party IT security firm or tool may be contracted/utilized to assess and recommend modifications to CSUF Firewall Policies/Rules, Objects, and Group Categories for relevance and correctness.

Whenever a request for Firewall Policies/Rules is received through the IT Help Desk Ticketing System (Service-Now) for a server or service application requiring direct access from the Internet the following information must be included:

1. Server(s) or Application Name (Service Application Owner)
2. Request for Routable IP Address(es) (Service Application Owner)
3. Ascertain and fully understand the customer/client requirements or use case(s) (Service Application Owner and IT Network Team)
4. Required technical requirements (Service Application Owner)
5. Load Balancer (SSL Cert, Multiple server or cluster)
6. Port(s) to be Allowed
7. Rationales for needing this police come from (Service Application Owner)
8. DNS name (CNAME, Alias)
9. Scan Server(s)/Application(s) for vulnerabilities using campus vulnerability management system (ISO Team)
10. Assign External (Routable) IP Address (IT Network Team)
11. Change Management Approved (ISO)
12. Create or Modify and Apply to appropriate Firewall Policy/Rule (IT Network Team)
13. Update external DNS (IT Network Team)
14. Validate with Service Application Owner
15. Test DNS Name resolution (IT Network Team)
16. Require testing by Service Application Owner
17. Verify actual port usage in Firewall Logs (IT Network Team)
18. Make appropriate adjustment as necessary (IT Network Team)
19. Add or Modify Comments Field with date of entry, purpose, and initials of firewall technician (IT Network Team)

G. UNIVERSITY OWNED MOBILE DEVICE MANAGEMENT

Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:

1. Specific configuration settings are defined.
2. Personal firewall (or equivalent functionality) is actively running.
3. Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

See Appendix B on ICSUAM 8045.S400, Guidelines on CSU mobile device

STORAGE OF PROTECTED DATA

1. Campus prohibits storage of protected Level 1 data on a mobile device.
2. IT Rollout Services must maintain a current inventory of mobile devices that contain protected Level 1 data. This inventory must be reviewed at least annually. However, some mobile devices are directly purchased at the department level, hence, will not be included in the Rollout list.

USER PRACTICES FOR MOBILE DEVICES

Departments must complete IT-Purchase Request Authorization for any hardware or software products. The form includes request for information that stores, process, or transmit cardholder data. If a department confirms that system will be used to process, store or transmit cardholder data, ISO and ISA are immediately notified for PCI requirements compliance.

Recipients of laptop computers and mobile devices must complete a Wireless Authorization Form Work Order through Titan Service Now. All requests are reviewed and approved by department head and configured by Information IT Rollout Department (see IT Rollout for more information)

IT Rollout Services and department technician apply the CSU minimum requirements and must meet Common Workstation Standards (ICSUAM 8050.S100). All mobile devices that meet the High Risk Designation shall include the following configurations:

1. Network Protection
2. Protection against “zero day” malware
3. Host-based Firewall
4. Security Event Logging
5. Administrative Accounts
6. Encryption

7. Remote Support
8. High Security Workstation Configuration Checklists
9. Vulnerability Scanning
10. Peripheral Communications
11. Campuses Property Assets Tag

Campuses must maintain and publish a process for users to report if they determine or suspect that any mobile device (including those not provided by campus) which enables access to non-public campus information assets has been lost, stolen, or compromised.

Employee signs Property Custody Receipt of each device released by university. Receipt includes device's Property Number or Serial Number. Employee is responsible for the security and maintenance of the property as part of their assigned duties for performance evaluation purposes. Employee must return the device to the department head or designated custodian and complete the "Return of the Property" section of the Property Custody Receipt.

It is the faculty/staff member's responsibility to take appropriate precautions to prevent damage to or loss/theft of his or her iPad/laptop. CSUF/IT will not repair or replace this iPad/laptop unless the cost of repair/replacement is paid by either the Department or the individual user. Any lost or stolen mobile device must be reported to IT Helpdesk immediately, and complete a loss form and police report in the event of a theft.

IV. REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

A. APPLICATION DEVELOPMENT

(ICSUAM 8070.S0, SECTION 1.5)

Application and web development environments must comply with CSU and campus standards and procedures. Contracts for services involving application, web development or hosting must incorporate appropriate language (see 8040.S000 Third Party Contract Language).

B. APPLICATION DEVELOPMENT AND PRODUCTION ARCHITECTURE

Development and testing must be performed in a non-production environment.

1. Production environments for applications with "high risk" (workstation/server that stores or accesses "critical" data or systems) should run on stand-alone dedicated servers or VM server containers.
2. Production servers and development servers, used to facilitate e-commerce activities must be housed in a data center isolated from regular university network per PCI Requirement 1, and

meets physical and logical security control requirements as per CSU Information Security Policy 8080 Physical Security.

3. Servers must be placed in the appropriate network zone based on the campus approved network architecture plan as per 8045.S4301 Boundary Protection and Isolation Standard § 2.2.
4. Servers should be "hardened" according to the campus configuration procedures in order to ensure that they are secure.

C. APPLICATION STANDARDS

Campus prohibits the following:

1. Except for P2PE solution, any local applications that transmit and or process credit card data over a network.
2. Use of campus wireless network with University owned Merchant IDs

D. APPLICATION CODING

Applications must be reviewed, tested, and documented as determined by a risk assessment, before being placed into a production environment to ensure vulnerabilities are addressed, including but not limited to:

Application Coding

a. Un-validated input
b. Injection flaws
c. Inadequate access control
d. Improper error handling
e. Inadequate authentication and session
f. Insecure storage
g. Cross-site scripting (XSS) attacks
h. Denial of service Standards
i. Buffer overflows
j. Insecure configuration

The integrity and availability of source code and/or critical files/folders must be ensured by use of a source code control system and scheduled backups.

E. SERVERS AND WORKSTATIONS IN PCI SCOPE

Division of Information Technology establishes configuration management standards to address information security risks on campus server, desktop and laptop computers (workstations) along with associated devices, which may store data, including the following:

1. 8050.S200 Configuration Management – High Risk Workstation Standard
2. 8045.S300 Configuration Management – Mobile Device Standard

Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and application servers should be implemented on separate servers.)

Where virtualization technologies are in use, implement only one primary function per virtual system component.

Enable only necessary services, protocols, daemons, etc., as required for the function of the system (ICSUAM 8045.S301).

Campus IT Server & Storage Support maintains guidelines in hardening servers (i.e., Linux, Windows & VMWare Infrastructure).

Campus IT Client Rollout Support service maintains guidelines in hardening rollout workstations and laptops.

Configure system security parameters to prevent misuse.

Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, server services, and unnecessary web servers.

Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

Shared hosting service providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed CSU General and Supplemental Provisions contract language.

V. REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

Campus prohibits the storage of sensitive credit card data. Sensitive credit card data includes, but it not limited to:

1. Sensitive Authentication Data (SAD)
2. Credit Card Number (PAN)
3. Personal Identification Number (PIN)
4. Full Magnetic Track
5. Card Verification Code (CVC)

VI. REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

A. SECURING ECOMMERCE

Electronic commerce, commonly known as e-commerce, is the use of the Internet to facilitate transactions for the sale and payment of goods and services. E-commerce is a card-not-present (CNP) payment channel and may include:

1. E-commerce websites accessible from any web-browser, including "mobile-device friendly" versions accessible via the browser on smart phones, tablets, and other consumer mobile devices

2. "App" versions of your e-commerce website, i.e., apps downloadable to the consumer's mobile device or saving of the URL as an application icon on a mobile device that has online payment functionality (consumer mobile payments)

An e-commerce solution comprises the software, hardware, processes, services, and methodology that enable and support these transactions. Merchants choosing to sell their goods and services online are limited to the following e-commerce implementations:

B. SHARED-MANAGEMENT

1. URL redirection to a third-party hosted payment page – the cardholder is redirected from the merchant's website to a third-party page. The cardholder then enters their account data into a payment page hosted by the third-party payment service provider (PSP).

THE REDIRECT PROCESS

See Appendix C, Figure 1, Diagram of Redirect Process

   a. Merchant website sends a redirect command to the customer's browser.
   b. The customer's browser then requests a payment form from the PSP.
   c. The PSP creates the payment form and sends to the customer's browser.
   d. The customer's browser displays the PSP's payment form.
   e. The customer enters account data and sends to the PSP.
   f. The PSP receives the account data and sends it to the payment system for authorization

2. An Inline Frame (or "Iframe") that allows a payment form hosted by a third party to be embedded within the merchant's web page(s)

THE IFRAME PROCESS

See Appendix C, Figure 2, Diagram of Iframe Process

   a. The merchant website creates an Iframe within the current webpage. The customer's browser requests the payment form from the PSP.
   b. The PSP creates a payment form and sends to the customer's browser within the Iframe.
   c. The customer's browser displays the payment form within the Iframe located on the merchant page.
   d. The customer enters their payment details into the Iframe containing the PSP's payment form.
   e. The PSP receives the account data and sends it to the payment system for authorization.

3. Wholly outsourced e-commerce implementations

C. EXCLUSIONS

The university prohibits the following options:

1. Proprietary/custom-developed shopping cart/payment application

2. Commercial shopping cart/payment application fully managed by the merchant/university
3. Data storage - encrypted or not
4. Use of GSM, CDMA, GPRS, Satellite communications & wireless technologies, including 802.11 and Bluetooth on university owned devices.
5. Shared-management e-commerce utilizing the following:
   a. Embedded content within the merchant's page(s) using non-Iframe tags.
   b. Direct Post Method (Form)
   c. JavaScript Form
   d. Merchant gateway with third-party embedded application programming interfaces (APIs) or Electronic Data Interchange (EDI)

VII. REQUIREMENT 5: USE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

PREVENTION OF THE INSTALLATION OF MALWARE (MALICIOUS CODE)

Virus, spyware, and other malware definitions are files that are used to identify malicious or potentially unwanted software. The university uses essential anti-virus software for PCI in-scope system components to automatically update these definitions.

Client Rollout Services standard policy is to install anti-virus software, on all computer workstations that are part of Cardholder Data Environment (CDE). Anti-virus mechanisms are actively running and cannot be disabled or altered by users. However, users can scan their computer on demand.

Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by Information Security Officer (ISO) on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized through Help Desk (ext. 7777). Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.

The university has strict guidelines in the prevention of the installation of malware. Each facility must implement steps to prevent malicious code from being installed and executed on the computers. In lieu of this, each facility needs to have a documented procedure for installing security updates, monitoring for security threats, and remediation of problems that occur in computers.

VIII. REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

A. AREA OF RESPONSIBILITIES

1. *Information Security Team* – The basic role of the security team is to configure the scanning tool, run scans, prepare, review and disseminate reports, and provide assistance.
2. *Application Management* – Management staff who are responsible for assigning individuals to review the scan report approve remediation and provide documentation to determine acceptable risk.

3. *Application Teams/Infrastructure Services* – Staff will review potential vulnerabilities and implement remediation recommendations. As appropriate, staff may take steps to reclassify, provide documentation and business justification to demonstrate vulnerability as false-positive or an acceptable risk.
4. *Infrastructure Services* – In addition to remediation responsibilities, Infrastructure Services staff & department technicians will complete monthly patching according to the established schedule.

B. METHODS FOR EVALUATING VULNERABILITIES

1. *Critical risk* – vulnerabilities that pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed
2. *High risk* – vulnerabilities that have potential threat to the Cardholder Data Environment (CDE)
3. *Acceptable risk* – vulnerabilities with compensating controls in place to mitigate the risk, or risk is identified as critical but is accepted and approved.
4. *Acceptable risk exceptions* – Vulnerabilities that are recognized and it is determined that the risk is so low that it accepted and no further action is needed; or the financial cost of remediation is so great that it is not feasible to make changes to alleviate the vulnerability.
5. *Data Owner* – Management staff who approve access and changes to information/data of an application.
6. *Data Steward* – The individuals who make up the application teams and have the best ability to verify vulnerabilities and make recommendations for remediation.
7. *False-positive* – Vulnerabilities identified in the scan that are not vulnerabilities and do not cause a threat to the CSUF systems.

C. PROCEDURES

Step 1 – Run Scans and Prioritize Findings

ISO staff quarterly scan internal and external PCI in-scope system components and software. ASV approved by PCI SSC performs annual run of penetration testing using intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusion into the network. The reports list vulnerabilities as critical, severe and moderate. Scan reports are prioritized based on vulnerabilities with focus on critical/severe and high risk for immediate remediation. Moderate vulnerabilities are remediated when time is available. PCI requirements calls for remediating Critical and Severe vulnerabilities within 30 days.

ISO staff identify the risks associated with critical/severe and high-risk vulnerabilities and distributed to appropriate areas of responsibilities.

Step 2 – Review Reports of Vulnerabilities

ISO meet with application teams to discuss result and provide guidance or explanation of the findings. Correct any exploitable vulnerabilities found during penetration testing and repeat testing to verify corrections (See Appendix D)

Step 3 – Apply Patches

Patches are applied on a monthly basis as follows:

a. Infrastructure Services staff will identify needed patches and submit a change request (CR) for approval.
b. Infrastructure Services staff will install patches in the development and test environments on the Thursday following the release of Microsoft patches.
c. Patches to the production environment will be installed on the following Sunday at 12:00 a.m.

Note: PCI Requirement 11.2 requires quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

IX. REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

Access to system components and software within the cardholder data environment must be controlled and restricted to those with a business need for that access. The University achieves this through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a need to know.

To ensure cardholder data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need-to-know and according to job responsibilities.

Need-to-know refers to when access rights are granted to the least amount of data and privileges needed to perform a job (least privileges model).

A. LIMIT ACCESS TO CARDHOLDER DATA

Access to cardholder data and system components in the cardholder data environment must be restricted to only those individuals whose job requires such access.

Access limitations must include:

1. Restriction of access rights of privileged user IDs to least privileges necessary to perform job responsibilities.
2. Assignment of privileges based on individual personnel's job classification and function.
3. Requirement for a documented approval by authorized parties specifying required privileges.
4. Implementation of an automated access control system.

B. RESTRICT ACCESS TO NEED TO KNOW

Establish an access control system for systems components in the cardholder data environment with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:

1. Coverage of all system components in the cardholder data environment.
2. Assignment of privileges to individuals based on job classification and function.
3. Developer access should be limited to the least privilege necessary for development
4. Each application process should execute with the least set of privilege necessary to complete the job

C. ENCRYPT PROTECTED INFORMATION

Applications must encrypt Protected Level 1 information as it is transmitted over the network, including login credentials and session identifiers as per 8065S000 § 12.3 The SSL/TLS (Secure Sockets Layer) protocol is the CSU standard for protecting web-based network traffic. Certificates must be used to provide positive identification of applications to users. Servers must have valid certificates, signed by a recognized Certificate Authority

X. REQUIREMENT 8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

A. PURPOSE

The purpose of this guideline is to establish a standard for account use and creation of strong passwords which adheres to CSU policy and conforms to NIST Level of Assurance 2 requirements.

Division of Information Technology establishes university password policy for students, faculty & staff to access campus portal. See IT website

B. USER ACCOUNT USAGE, DELETION, SUSPENSION OR TERMINATION

Accounts assigned to employees are subject to deletion immediately upon termination of employment unless prior arrangements have been made and approved by the former employee's supervisor.

Accounts assigned to students are subject to deletion one hundred eighty days after graduation or withdrawal from the University unless specific arrangements have been made and approved by the Office of Student Affairs.

Assigned accounts may be suspended (i.e., inaccessible to the user) immediately and temporarily under three circumstances:

1. Upon recommendation of the appropriate judicial body in writing or email sent to the Vice President of Information Technology or Information Security Officer;
2. When Information Technology staff responsible for systems management have credible evidence that continued use of an account constitutes a threat to the integrity, security, or functionality of

computing systems, or to protect the University from liability. Every reasonable effort will be made to notify the Vice President of Information Technology as soon as possible of any such suspension.

3. When the account is inactive for 180 (one hundred and eighty) days or more.

Assigned accounts may be terminated immediately and permanently upon the recommendation of the appropriate judicial body in writing or email sent to the Vice President of Information Technology. An individual whose assigned account has been permanently terminated may not seek to have a new account assigned to them without approval of the appropriate judicial body.

Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with the Information Security Office.

Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

C. MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires that the factors be different in type. That is, at least two of the usual three types given below are required:

1. Something you know (e.g., password, PIN, security question challenge)
2. Something you possess (e.g., ICC card, physical token, cryptographic token or private key)
3. Something you are (e.g., physical biometric or behavioral biometric)

These factors must be independent. Access to one should not grant access to the other. For example, if mobile phone device is used for logging into a system, and the system can validate the device with a high-degree of assurance, then it's something you possess. However, if it is also where the password is stored (or the device to which a one-time-password (OTP) or password reset would be sent), then possession of the device may grant access to both factors, therefore losses independence.

University shall follow a high-degree of digital authentication that requires a higher level of capabilities or resources on the part of an attacker in order to successfully authenticate, effectively reducing the risk of authentication error. Current campus MFA policy follows NIST requirements on Digital Authentication methodology. See Nist Publication SP 800-63

University personnel with administrative access to in-scope system components (see Firewall Policy – Scoping Concept) are required to use MFA.

XI. REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

ICSUAM 8080.S01

Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to campus' information assets. Campus controls must be adequate to protect critical or protected data. Such controls must:

1. Manage control of physical access to information assets (including personal computer systems, computer terminals, and mobile devices) by campus staff and outsiders.
2. Prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failure.

A. SECURITY ZONES

Division of Information Technology assigns an appropriate security zone designation to their physical areas. Appropriate physical controls must be implemented in shared and limited access security zones to manage access. These controls are reviewed regularly.

Zone	Brief Description	Necessary Controls
Public	No information assets containing protected data or critical systems are located in the area. (Example: Student Union, Library open areas)	None. Access to this area are unrestricted.
Shared Access	An area containing one or more protected information assets or critical systems. Persons in the area include those who do not have authorization to protected information assets or critical systems stored in the area. (Example: Administrative Offices)	Appropriate physical access controls and construction must be implemented to restrict access to protected information assets or critical systems that reside in the area.
Campus Limited Access Area	An area containing one or more protected information assets or critical systems. Persons in the area are authorized to access the protected information assets or critical systems. (Example: Data Center)	Appropriate physical access controls and construction must be implemented that limit access to the area to only persons having a need for specific access in order to accomplish a legitimate task. The controls must enforce the principles of need to know and least possible privilege. All physical access to such areas must be controlled by mechanisms such as tracking and logging. Access records must retain information such as: • Records identifying persons with keys (credentials, etc) • Where possible, systems must provide ➢ Date and time of access ➢ User ID performing access

B. ENVIRONMENTAL CONTROLS

University Data Center has processes and facilities in place to prevent, detect, suppress fire, water damage, air flow, cooling, and loss or disruption of operational capabilities due to electrical power fluctuations or failure. All authorized personnel must familiarize themselves with any data center controls to prevent any accidental power loss, cooling mishap or fire suppressant discharge by attending a data center safety course. Contact the lead data center coordinator for data center safety course.

C. ROLES AND RESPONSIBILITIES

1. It is the responsibility of all employees with access to protected information to adhere to these guidelines.
2. It is the responsibility of all department managers to ensure that employees in their department adhere to these guidelines.
3. It is the responsibility of Campus Data Center staff to assure that these guidelines are followed.

D. DATA CENTER AUTHORIZED ACCESS

Access to campus Data Centers is normally granted on a need only basis, and is granted only after a Data Center Access Request Authorization Form is completed. The form undergoes approval process as follows:

1. employee's appropriate Administrator,
2. Information Security Officer (ISO)
3. Associate Vice President – IT
4. CITO Delegate

An employee who has been granted approval for access to Data Center is provided with a copy of the Data Center Access Guidelines and Confidentiality Agreement. ISO maintains all completed and signed request forms. The list of individuals granted access to the Data Center shall be reviewed, annually. All individuals given Data Center Access shall receive a copy of this policy. Employees who leave the service of the University or who change roles within the University and no longer require access shall have their access terminated immediately.

E. AUTOMATED ACCESS – NUMERIC KEYPAD, KEY OR KEYCARD (CARD SWIPE) HOLDERS

Key, card swipe is required to enter the data centers during campus business hours or can be arranged during non-business hours for authorized users. Access is limited only to authorized personnel who have network and server systems responsibilities, Facilities & Maintenance employees and campus Public Safety Department staff. **Vendor Access**

An approved vendor list should be maintained at the data center. With proper notification and justification, approved vendors will be allowed into the data center to perform scheduled maintenance or repair work. Vendors with approved access to the Data Center are required to identify themselves and sign in/out of the Data Center using a Site Access Log located within the Data Center.

F. OCCASIONAL ACCESS

Employees who need only occasional access shall be treated as not having a need for access. Occasional access will be allowed during normal campus business hours and these individuals will require an IT escort.

Visitors who are allowed access to Data Center are entered into the log sheet and are accompanied by authorized personnel and do not need to complete the Data Center Access Authorization Form.

G. DATA CENTER MACHINE ROOM ETIQUETTE

In order to maintain a clean room environment and allow all work performed in the Data Center to be carried out as efficiently as possible, it is mandatory for all persons working within the Data Center machine room to adhere to the following rules of etiquette:

1. All work areas must be kept clean and free of debris. Upon completion of any work in the room, staff performing the work should ensure they have left the area as clean as it was before their work began.
2. All rack enclosures should be kept neat and free of manuals, diskettes, cables, etc. Doors on all racks should remain closed at all times except during performed work.
3. Cables should never be strung outside of rack enclosures. Cabling between rack enclosures of adjacent racks is accepted provided sufficient pass-through chassis are in place.
4. Under no circumstances should any visitor:
    a. Lift floor tiles without prior knowledge, consent, and oversight of the Data Center Operations staff.
    b. touch a Power Distribution Unit (PDU) within the Data Center,
    c. touch a Computer Room Air Conditioning Unit (CRAC) within the Data Center,
    d. Open a Data Center communications cabinet, i.e. an RCR or DCCR.
    e. Plug any device into another cabinet's power supply.

H. PHYSICAL LOCATIONS OF TERMINALS AND TERMINAL INFRASTRUCTURE SECURITY

1. TERMINALS

a. Design all terminals payment location with intent to control customer access to payment technology and the payment location. Designs should include the protection and security of equipment and the respective cables and power sources. Security should extend into the ceiling and below flooring levels of the payment location, when applicable

b. Mount and secure the terminal and cables with locking stands, cable trays, and other securing mechanisms

c. Position the PIN entry device so there is no method of actually being capable of recording or viewing any PIN entered by employees, students or others

d. Leverage current PCI SSC standards and practices for terminals, terminal infrastructure, and the payment card data they process

e. Place payment terminals and technology in a manner that offers the greatest level of security

f. Physically secure and alarm all remote or self-service terminal payment environments to the greatest extent possible. Use long-standing retail physical security concepts (facility and site lighting, facility and site access, physical security systems, security operations and checks, etc.) to complement payment locations and support terminal security needs. Focus specifically on unattended terminals and payment locations to prevent skimming attacks.

g. Maintain a list of all devices

h. Develop a schedule or routine to inspect devices to look for tampering or substitution. This could be once a day or at the beginning of each shift

i. Report tampered or substituted devices to Help Desk, immediately

j. Train personnel to be aware of suspicious behavior of customers and to report tampering or substitution of devices immediately as outlined in the incident response plan.

k. Periodically rotate the individuals performing the device-checking to ensure nothing gets missed and to eliminate collusion

2. TERMINAL INFRASTRUCTURE

a. Secure terminal wiring and communication lines with conduit or within physical structures of the facility when allowed or required by local building codes. Limit exposed terminal cable and wire or non-secure channels for communication infrastructure when possible. The intent should be to make it as difficult to access terminal wiring and cabling as possible, requiring more time on site to tamper or compromise terminal cabling.
b. Protect all telephone rooms, panels, routers, drops, and connections that support terminal infrastructure. Use locks and control access to sensitive electrical and telephone closets that support payment infrastructure. Conduct regular checks of this infrastructure as required with management and security staff trained to be on the lookout for compromises.
c. Segment and protect card data network from other functions within the merchant environment that may have access to public or other networking environments as outlined in PCI DSS.
d. Protect access to wireless infrastructure such as Bluetooth and Wi-Fi and control access to wireless routers, passwords, and SSIDs. Leverage PCI SSC standards and practices for password and access controls.
e. Whenever possible, encrypt the cardholder data leaving the terminal.

3. CAMERAS, PLACEMENT, ACCESS, AND IMAGE STORAGE

a. Use appropriate lighting as required to support payment environments and the monitoring capabilities of surveillance cameras. Ensure Kiosks are well lighted and meet minimum physical requirements as defined by the appropriate regulatory mandates.

b. The surveillance cameras should be sited such that they record the area around the PIN entry device but allow no method of actually recording or viewing any PINs entered.

c. Support PCI DSS guidelines for 90-day storage of surveillance images
d. Locate cameras to cover primary site entrances and facility entrances. Use surveillance cameras to monitor payment lanes and locations when possible. Facility cameras provide a level of deterrence and a record of activity that can be used to support investigations.

e. Immediately examine all terminals if a camera has been moved, damaged, or if images have been blocked. This may be an indicator that criminals have targeted your merchant location.
f. Note the following:
    1) Time stamps—in case the camera was switched off for a period of time
    2) Any blackouts
    3) Any period when the surveillance cameras image is blocked
    4) Any incident when the camera is moved

XII. REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

Important components of overall system security for the cardholder data environment are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The University must address system monitoring and vulnerability testing using the following policies:

TRACK AND MONITOR ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs, and the University will maintain such logs according to the following:

1. *ESTABLISH AN AUDIT PROCESS*

   Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

2. *IMPLEMENT USER-BASED AUDITING*

   Implement automated audit trails for all system components to reconstruct the following events: (PCI DSS Requirement 10.2)
   a. All individual accesses to cardholder data.
   b. All actions taken by any individual with root or administrative privileges.
   c. Access to audit trails.
   d. Invalid logical access attempts.
   e. Use of identification and authentication mechanisms.
   f. Initialization of the audit logs.
   g. Creation and deletion of system-level objects.

3. *LOG SYSTEM EVENTS*

   Record at least the following audit trail entries for all system components for each event:

a. User identification
b. Type of event
c. Date and time
d. Success or failure indication
e. Origination of event
f. Identity or name of affected data, system component, or resource

4. *SYNCHRONIZE SYSTEM CLOCKS*

Using time-synchronization technology (for example, network time protocol), synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time:

a. Critical systems have the correct and consistent time.
b. Time data is protected.
c. Time settings are received from industry-accepted time sources.

5. *SECURE AUDIT TRAILS*

a. Secure audit trails so they cannot be altered
b. Limit viewing of audit trails to those with a job-related need
c. Protect audit trail files from unauthorized modifications.
d. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
e. Write logs for external facing technologies onto a log server on the internal LAN.
f. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed with generating alerts (although new data being added should not cause an alert).

6. *REVIEW AUDIT LOGS DAILY*

Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection systems (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.

7. *RETAIN AUDIT TRAIL HISTORY*

Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restored from back-up).

XIII. REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

A. PENETRATION TESTING

The university uses a PCI Approved Scanning Vendor (ASV) with approved tools to conduct internal and external vulnerability services. The scanning vendor's ASV scan solution is tested and approved by PCI SSC.

Using tools and application provided by PCI ASV provider, vulnerability scans are performed quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

PCI ASV provider performs penetration testing, annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment) that includes the following:

1. Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
2. Includes coverage for the entire CDE perimeter and critical systems
3. Includes testing from both inside and outside the network
4. Includes testing to validate any segmentation and scope-reduction controls
5. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
6. Defines network-layer penetration tests to include components that support network functions as well as operating systems
7. Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
8. Specifies retention of penetration testing results and remediation activities results.

University Information Technology ensures that all PCI in-scope system components and software are protected from known vulnerabilities by installing applicable vendor supplied *critical* security patches (currently using BigFix and will soon switch to SCCM/WSUS, but all this is contingent on the clients being installed on the workstations. Also, on Apple devices, we haven't completed work to install MDM profile so critical patches are installed by user) within 30 days of release.

Critical patches should be identified according to industry best practices as well as consideration of potential impact.

B. REMEDIATION PROCESS

Remediation procedures are designed to ensure that University PCI system components and software are protected from any risk and vulnerabilities

Information Security Office (ISO) staff through PCI DSS certified ASV tools and application, identify potential threats and vulnerabilities, quarterly. ASV approved by the PCI SSC submits Pentest reports to the University, annually. The work to maintain a secure infrastructure environment is a collaborative effort between ISO, IT application teams and Infrastructure

XIV. REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

A. IMPLEMENT AN INCIDENT RESPONSE PLAN

(Requirement 12.9)

The University has issued DR-10 Fullerton-Incident Response Protocol in the event of a system breach. This ensures the following, at a minimum:

1. Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum:
    a. Specific incident response procedures.
    b. Business recovery and continuity procedures.
    c. Data back-up processes.
    d. Analysis of legal requirements for reporting compromises.
    e. Coverage and responses to all critical system components.
    f. Reference or inclusion of incident response procedures from the payment brands.
2. Test the plan at least annually
3. Designate specific personnel to be available on a 24/7 basis to respond to alerts
4. Provide appropriate training to staff with security breach response responsibilities
5. Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems
6. Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments

B. ACCESS AUTHORIZATION

Usage of “High Risk” or “Critical” technologies requires the following:

1. explicitly authorized
2. include multi-factor authentication for use of the technology
3. include list of all such devices and personnel with access
4. a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
5. acceptable uses of the technology
6. acceptable network locations for the technologies
7. list of university-approved products
8. automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
9. activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.
10. For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media,

unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirement

C. SECURITY AWARENESS

CSU Policy (ICSUAM 8045.S200) requires that each campus implement or adopt a program for providing information security awareness and training to employees which may be appropriate to their level of access to campus information assets. The campus Information Security Awareness Program must also promote campus strategies for protecting information assets containing protected data.

All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, Information Security Awareness Program must be provided to individuals whose job functions require specialized skill or knowledge in information security.

D. IT PURCHASING CHECKLIST

All university acquisition of electronic technology product/service completes and submits Security Data Requirement Checklist or Electronic & Information Technology (E&IT) Purchase Review via Service Now

Prior to the issuance of a contract, the IT Security Office must review requests involving any services requiring either access to or campus supplied CSU protected information. Since contracts and services can evolve over time, the checklist must be completed every contract revision or renewal to ensure compliance in securing data, systems and network. The completed checklist is submitted to the IT Security Office for review and signature. Approved checklist are forwarded to Contract and Procurement to proceed with the requisition.

For more information, visit IT Purchasing

XV. REFERENCES AND RELATED DOCUMENTATION

Integrated CSU Administrative Manual (ICSUAM), Section 3102.05 Debit/Credit Card Payment Policy

Integrated CSU Administrative Manual (ICSUAM), Section 8000, Information Security

Division of IT Purchasing Policy

CSU Data Classification of Level 1, 2 & 3 Data

PCI Security Standards Council

CSUF PCI DSS Website

CSUF Cash Management Policy

CSUF Merchant ID Request

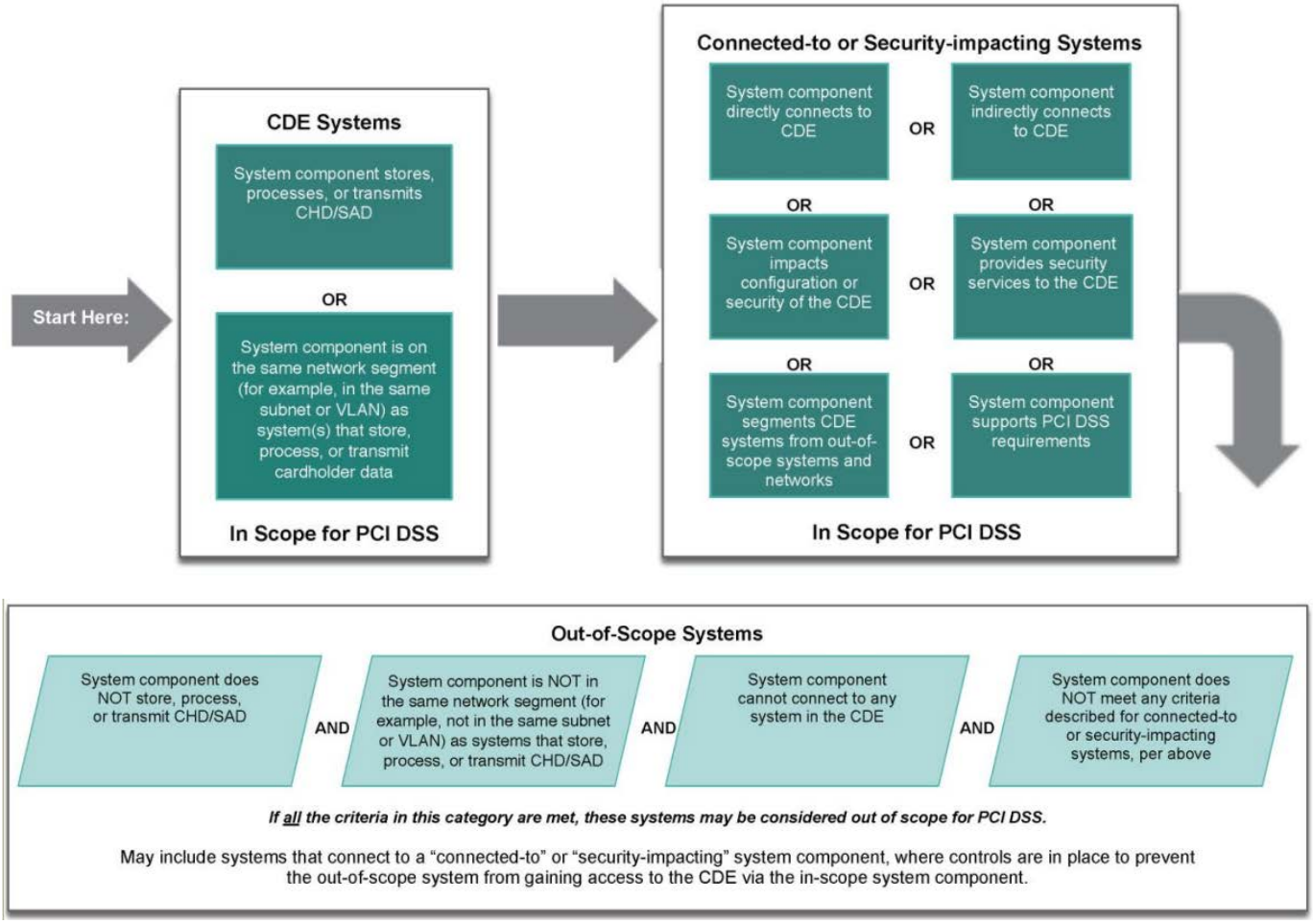
CSUF eMarket Site

HR Memo 2005-10

XVI. APPENDICES

APPENDIX A

FIGURE 1 – PCI DSS Scoping Categories



System components can be categorized into only one of these categories. These categories are hierarchical, with CDE Systems as the highest category that should be considered first; if a system meets any criteria in CDE Systems, it is a CDE system regardless of whether it also meets a description for a lower category. The next category includes connected-to and security-impacting systems; this category takes priority over and is evaluated before the out-of-scope systems category is considered. To be considered out of scope, a system must meet ALL the criteria of the out-of-scope category and NONE of the criteria of a higher category.

APPENDIX B

MOBILE DEVICE MANAGEMENT

Mobile devices as consumer electronic handheld devices (e.g., smart phones, tablets, or PDAs) that are solely dedicated to payment acceptance for transaction processing. These devices span a broad spectrum of features and functions ranging from cellular handsets that only support telephone functionality to “smart phones” and “tablets” that have a broader functionality.

Any risk that exists on a standard desktop or laptop computer may also exist on a mobile device. In addition, mobile devices may have a broader set of functionalities than standard desktop and laptop computers, resulting in more security vulnerabilities. Along with the standard communication methods of traditional desktop and laptop computers, mobile devices may also include multiple cellular technologies (e.g., LTE, CDMA and GSM), GPS, Bluetooth, infrared (IR), and near-field communication (NFC) capabilities. Risk is further increased by removable media (e.g., SIM card and SD card), the internal electronics used for testing by the manufacturer, embedded sensors (e.g., tilt or motion sensors, thermal sensors, pressure sensors, and light sensors), and biometric readers. Furthermore, vendor and network operator-level logging and debugging configurations may introduce additional risks.

An inherent risk with mobile devices is the fact that they are mobile. A mobile device with wireless connectivity allows it to be removed from a merchant’s location, which is usually assumed to be safe, and taken to a location that is convenient for the customer. This can provide benefits to the merchant but it also creates many security risks. One of the risks to the merchant is the ease for a criminal to steal such a terminal, modify it, and return it without anyone realizing it was gone. Since the mobile device has no fixed location, keeping track of it, a clear university responsibility, becomes more challenging. Incidents of POS fraud are first reported to University Helpdesk, then forwarded to Information Security Office for mitigation.

As determined necessary by risk assessment, mobile devices that will impact the security of card holder data must be protected with appropriate security controls.

Appropriate security controls shall include, but are not limited to:

a) Physical access control
b) Encryption
c) Strong passwords
d) Anti-virus software
e) Personal firewall

*Note: Use of android devices are prohibited to process, transmit or store cardholder data.

Firewall configurations include:

- Specific configuration settings are defined for personal firewall software
- Personal firewall software is actively running
- Personal firewall software is administrative maintained and monitored by IT Program Administrator and not alterable by users of mobile devices.

APPENDIX C

FIGURE 1, DIAGRAM OF REDIRECT PROCESS

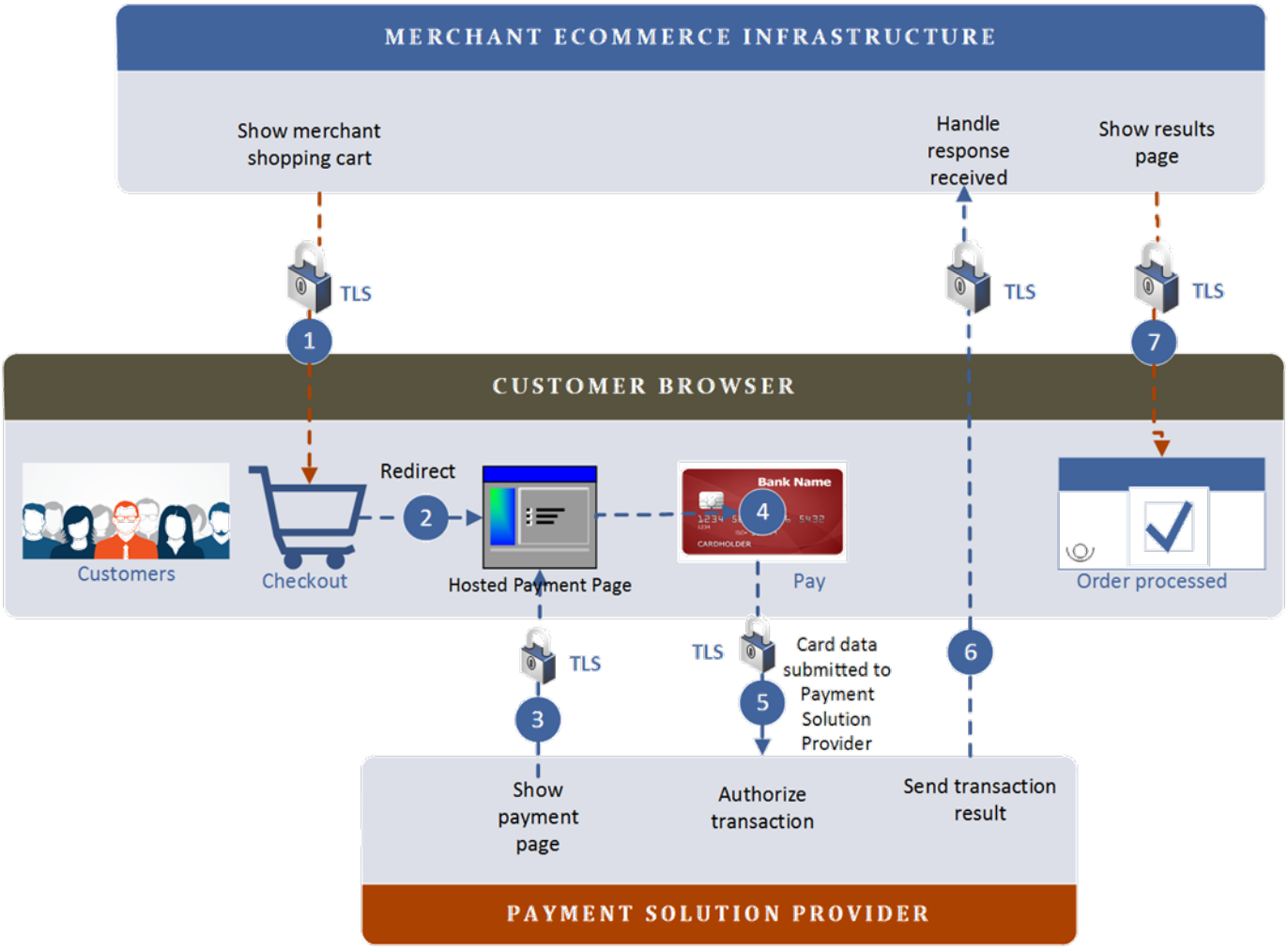
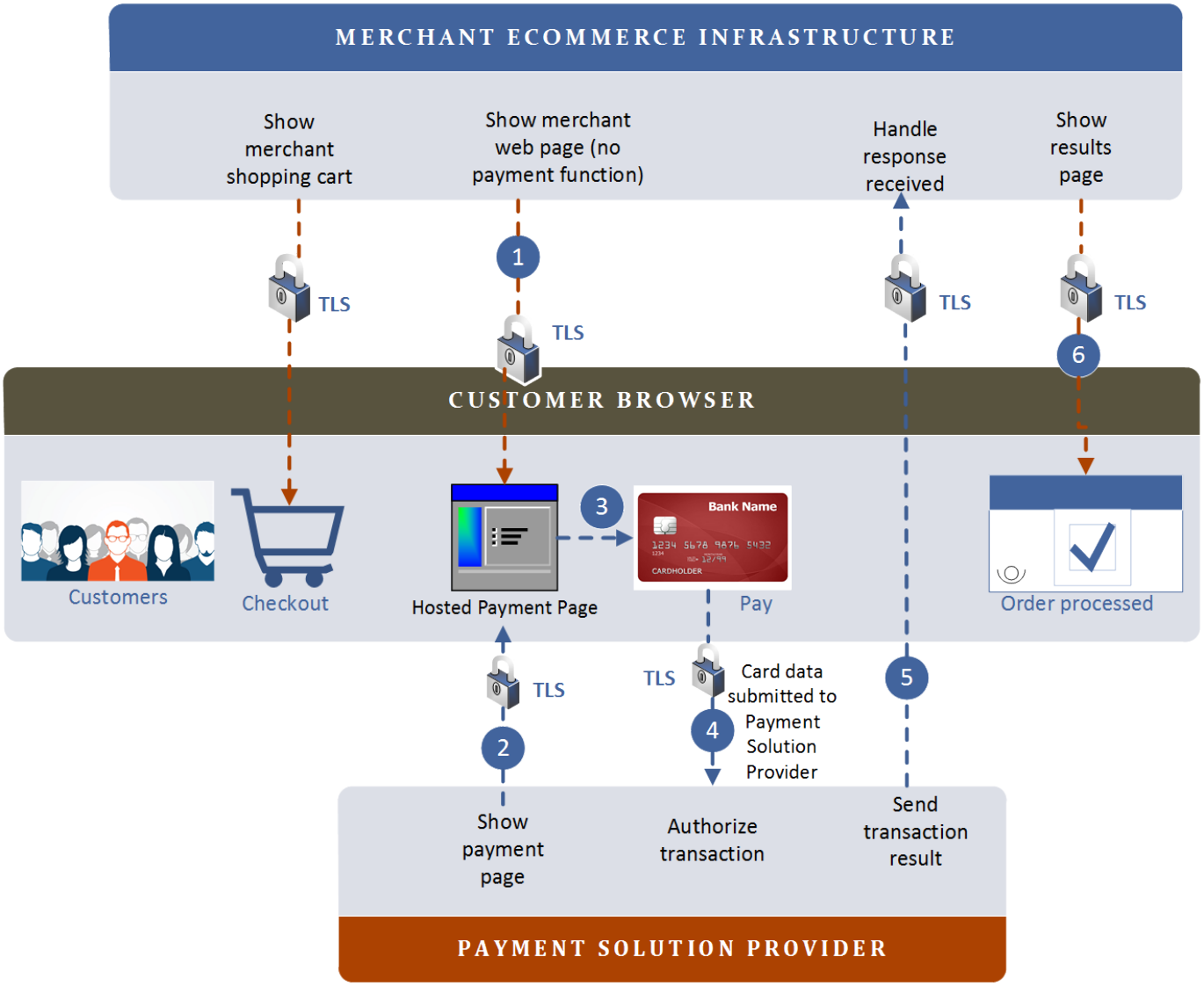
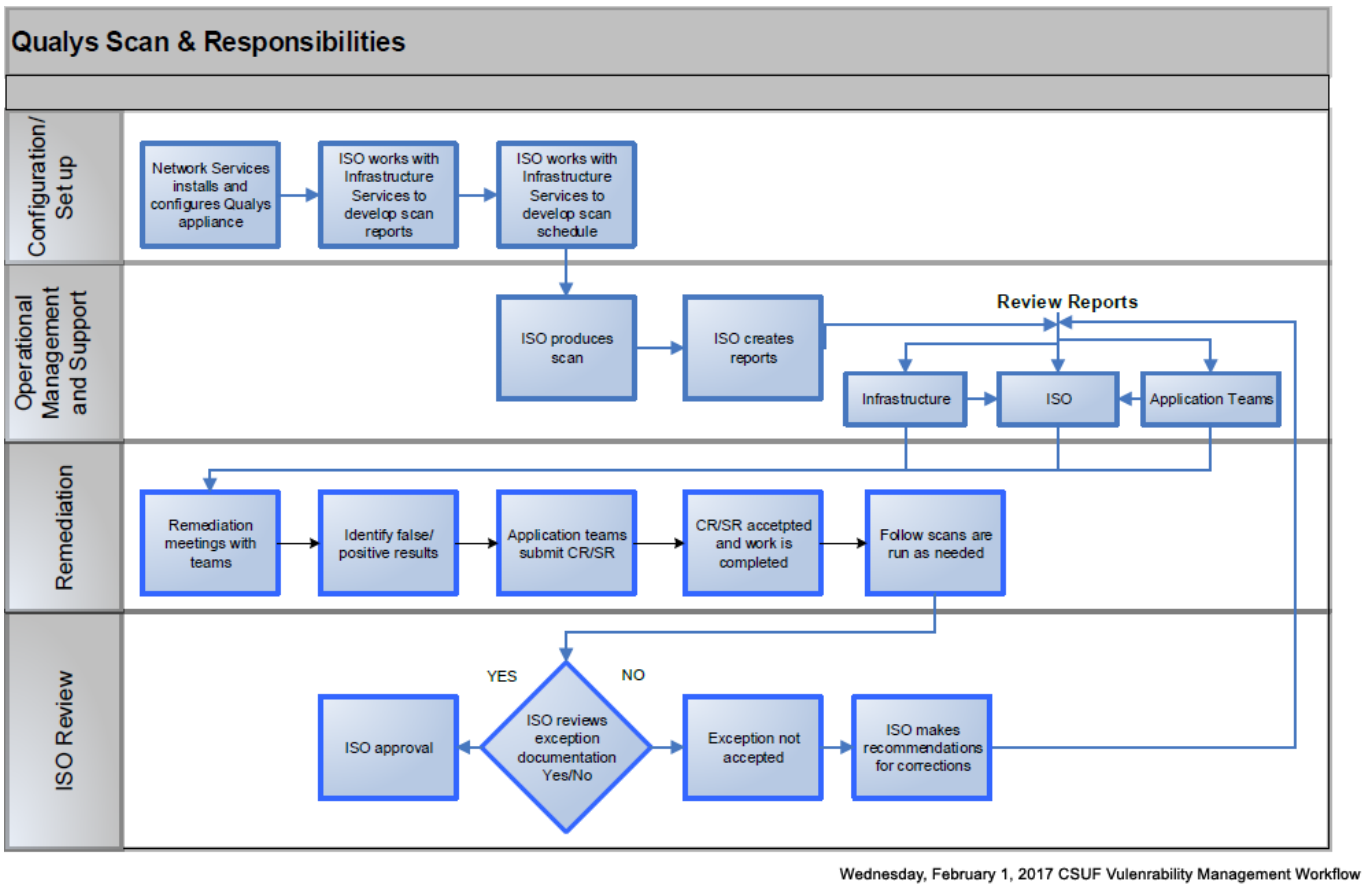


FIGURE 2, DIAGRAM OF IFRAME PROCESS



APPENDIX D



APPENDIX E

UNRESOLVED ISSUES AND VULNERABILITIES

(Not applicable to CDE)

If a vulnerability cannot be resolved through the normal patching process, ISO staff will suggest an alternative to alleviate the finding.

NOTE: The vulnerability continues to be recognized on reports until it is resolved.

On occasion, the data owner and ISO may determine a vulnerability cannot be resolved and the CSUF must recognize the exception as an acceptable risk. The data steward completes a *Security Risk Business Justification* form and submits it to ISO for approval.

In each of these cases, the CIO will be advised of the vulnerability and must approve the resolution.

APPENDIX F

IT Change Control Process

With quality and awareness in mind, the following are guiding policies:

1. Non-emergency changes to production hardware and software should be implemented during normal, scheduled downtimes, with adequate notice given to affected customers, and with appropriate consultation with stakeholders.
2. Major changes to hardware and software should only occur after careful review by IT technical and non-technical management.
3. Emergency Changes are ones that must be done immediately. It is of such a high priority that scheduling is not required. An example of an emergency Change might be the installation of new antivirus software during a period of severe viral infestation across the data center. Emergency Changes are ones that are typically not performed often. They are also referred to After the Fact Changes and will be reviewed by IT technical and non-technical management during next weekly Change Control meeting.
4. A formal control process will be used to assess change plans together in a forum that is conducive to effectively disseminating information to those who are potentially affected by a change. This process will be conducted consistently and conscientiously to ensure that changes are implemented in a timely fashion with little or no adverse impact on the campuses.
5. Change Management will be used to provide a historical trail of changes which are valuable in correlations and analysis of the relationships between system failures and/or performance problems.

Objective

The objective of Change Management is to ensure that standardized methods and techniques are used for efficient and prompt handling of IT changes, in order to prevent change-related incidents and avoid known issues by upgrading software. The objective is to make changes in such a way as to minimize negative impact on the delivery of services to users and clients.

Scope

This process applies to “Production” systems including:

1. network equipment and applications,
2. database systems and environments,
3. enterprise applications,
4. servers/systems/appliances,
5. desktop environments,
6. VoIP and analog telephone instruments and management systems,

7. security controls,
8. Other technology infrastructure equipment/systems in production.

Also this process applies to:

1. Systems/devices/applications/technologies that are transitioning to production.
2. Test environments, such as enterprise web test infrastructure, that are used by campus community for testing
3. Policies, process, procedures, architectures, tools, documentation and metrics
4. The scope of changes managed by this process may broaden or contract as the Change Advisory Board deems necessary.

Out of Scope

Operational level modifications to configuration items such as printer repairs, desktop/end-user hardware component replacement are considered outside the scope of Change management. Service request items such as add/move, create/delete user accounts are defined as routine changes but handled by the request fulfillment process.

Overview of the System

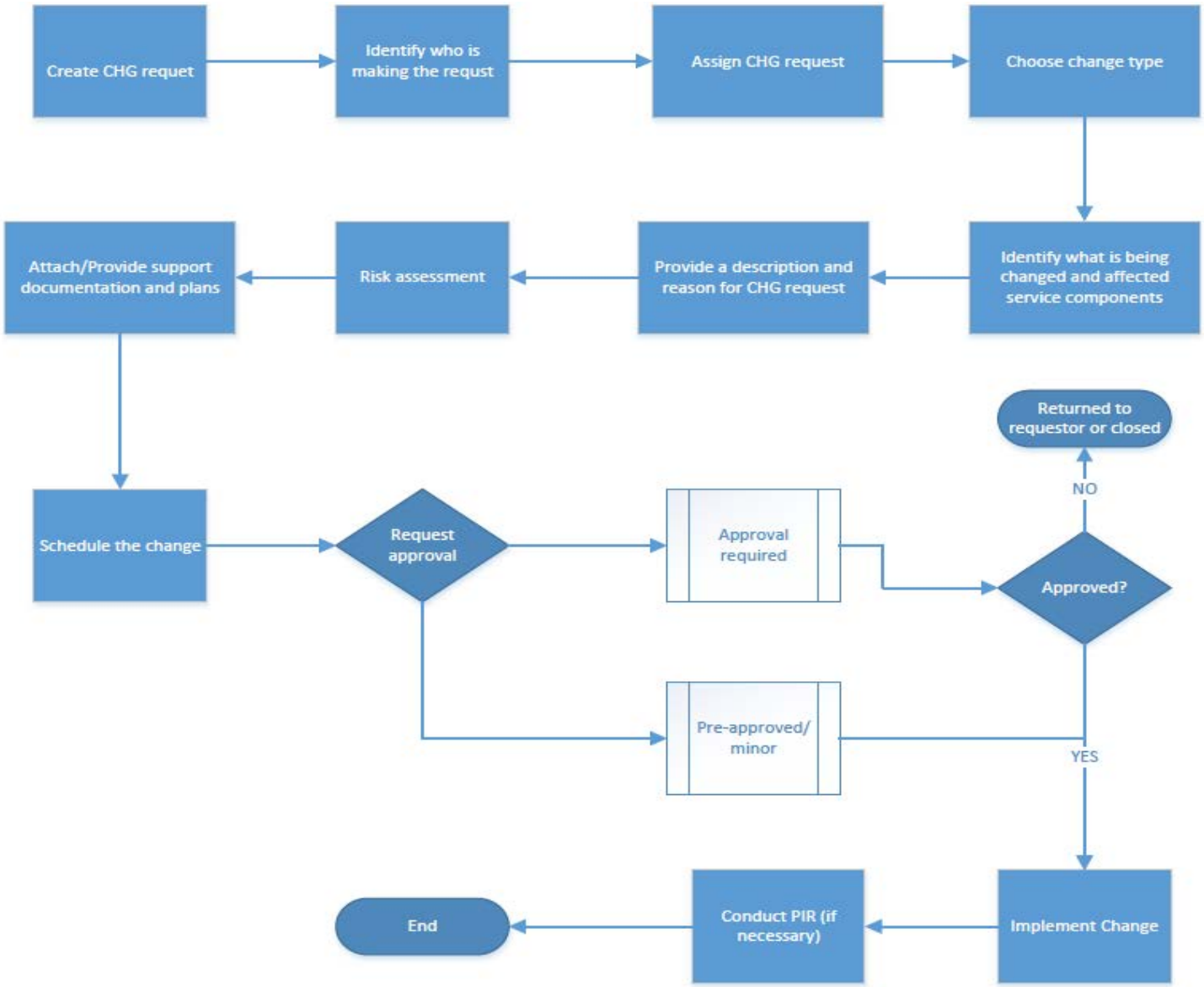
The Change Management process is comprised of seven (7) steps

1. Submit
2. Accept & Categorize
3. Assess
4. Authorize
5. Schedule
6. Implement
7. Closed

Detail elaboration of the Change Control Guideline discusses responsibility, activities & process is accessible in PCI Library Requirement 6, Change Control Process

APPENDIX G

HIGH LEVEL CHANGE MANAGEMENT DIAGRAM



XVII. GLOSSARY

TERM	DEFINITION
Access Control	Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.
Access to Critical Systems	An elevated access privilege2 to a system which stores protected level 1 information. Examples of this may include access to the Student Health System, access to payment card processing system, access to student financial records, etc.
Account Data	Account data consists of cardholder data and/or sensitive authentication data.
Account Number	See *Primary Account Number (PAN).*
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See also *Payment Processor.*
Administrative Access	Elevated or increased privileges granted to an account in order for that account to manage systems, networks and/or applications. Administrative access can be assigned to an individual's account or a built in system account. Accounts with administrative access are often referred to as "super user", "root", "administrator", "admin", "sysadmin" or "supervisorstate", depending on the particular operating system and organizational structure
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.

TERM	DEFINITION
AOC	Acronym for "attestation of compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or
Application	Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web)
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.
Audit Log	Also referred to as "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
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: a. Something you know, such as a password or passphrase b. Something you have, such as a token device or smart card c. 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	In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context 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.
BAU	An acronym for "business as usual." BAU is an organization's normal daily business operations.
BEQ	Acronym for Business Environmental Questionnaire that merchant must first submit prior to acquiring merchant ID

TERM	DEFINITION
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic processes 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: a. **CAV** – Card Authentication Value (JCB payment cards) b. **PAN CVC** – Card Validation Code (MasterCard payment cards) c. **CVV** – Card Verification Value (Visa and Discover payment cards) d. **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 unembossed 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: a. **CID** – Card Identification Number (American Express and Discover payment cards) b. **PAN CVC2** – Card Validation Code 2 (MasterCard payment cards) c. **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

TERM	DEFINITION
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.
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
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.
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.

TERM	DEFINITION
Console	Screen and keyboard which permits access and control of a server, mainframe computer or other system type in a networked environment.
Consumer	Students, parents or individual purchasing goods, services, or both.
Critical Data	includes protected level 1 information in such quantities as to require notification of a government entity (i.e. over 500 records under HIPAA or CA 1798.29), or information classified as protected level 1 due to severe risk
Critical systems / critical technologies	A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data. Considerations for determining which specific systems and technologies are critical will depend on an organization's environment and risk-assessment strategy
Cross-Site Request Forgery (CSRF)	Vulnerability that is created from insecure coding methods that allows for the execution of unwanted actions through an authenticated session. Often used in conjunction with XSS and/or SQL injection.
Cross-Site Scripting (XSS)	Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.
Cryptographic Key	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.
Cryptographic Key Generation	Key generation is one of the functions within key management. The following documents provide recognized guidance on proper key generation: • NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation • ISO 11568-2 Financial services — Key management

TERM	DEFINITION
	(retail) — Part 2: Symmetric ciphers, their key management and life cycle o 4.3 Key generation • ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle o 6.2 Key life cycle stages — Generation • European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management o o 6.1.1 Key generation [for symmetric algorithms] o 6.2.1 Key generation [for asymmetric algorithms]
Cryptographic Key Management	The set of processes and mechanisms which support cryptographic key establishment and maintenance, including replacing older keys with new keys as necessary.
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).
CVSS	Acronym for “Common Vulnerability Scoring System.” A vendor agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response. Refer to ASV Program Guide for more information.
Data-Flow Diagram	A diagram showing how data flows through an application, system, or network.
Database	Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets

TERM	DEFINITION
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
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." A system that stores information associated with domain names in a distributed database to provide name-resolution services to users on networks such as the Internet.
DSS	Acronym for "Data Security Standard." See PA-DSS and 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.)

TERM	DEFINITION
e-Commerce	The process of conducting payment transactions over a computer network, usually the Internet. In e-commerce, card-not-present, customers enter that cardholder data online.
Egress Filtering	Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the network.
e-Merchant	Merchant who uses e-commerce system to generate revenue
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	Also called “cryptographic 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.
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

TERM	DEFINITION
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
GSM	Acronym for "Global System for Mobile Communications." Popular standard for mobile phones and networks. Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed-length message digest. Hashing is a one-way (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 include an input variable (for example, a "salt") to the hashing function to reduce or defeat the effectiveness of pre-computed rainbow table attacks (see Input Variable). For further guidance, refer to industry standards, such as current versions of NIST Special Publications 800-107 and 800-106, Federal Information Processing Standard (FIPS) 180-4 Secure Hash Standard (SHS), and FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
High Risk	Workstation or server that stores or accesses "critical" data or systems.

TERM	DEFINITION
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.
HSM	Acronym for "hardware security module" or "host security module." A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data.
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.
ID	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 anomalies or 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 detected security events. See IPS
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.

TERM	DEFINITION
IMAP	Acronym for "Internet Message Access Protocol." An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
Index Token	A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information Security	Protection of information to ensure 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.
Injection Flaws	Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and Xpath injection.
Input Variable	Random data string that is concatenated with source data before a one-way hash function is applied. Input variables can help reduce the effectiveness of rainbow table attacks. See also Hashing and Rainbow Tables.
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 or authentication credentials (for example, 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 v1 and v2.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed and delivered from the source host to the destination host.

TERM	DEFINITION
	IP is the primary network-layer protocol in the Internet protocol suite. See TCP
IP Address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer (host) on the Internet.
LAN	Acronym for "local area network." A group of computers 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	Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.
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.
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
MAC	In cryptography, an acronym for "message authentication code." A small piece of information used to authenticate a message. See Strong Cryptography.

TERM	DEFINITION
MAC Address	Abbreviation for "media access control address." Unique identifying value assigned by manufacturers to network adapters and network interface cards.
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 or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Such software typically enters a network during many business
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.
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 four members of PCI SSC (American Express, Discover, MasterCard or Visa) as payment for goods and/or services.
MFA	See Multi-Factor Authentication
MID	Merchant ID, required to establish new payment processing
MO/TO	Acronym for "Mail -Order/Telephone-Order."
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.

TERM	DEFINITION
MPLS	Acronym for "multi-protocol label switching." Network or telecommunications mechanism designed for connecting a group of packet-switched networks.
Multi-Factor Authentication	Method of authenticating a user whereby at least two factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
NAC	Acronym for "network access control" or "network admission control." A method of implementing security at the network layer by restricting the availability of network resources to endpoint devices according to a defined security policy
NAT	Acronym for "network address translation." Also 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, allowing an organization to have internal addresses that are visible internally, and external addresses that are only visible externally
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 Diagram	A diagram showing system components and connections within a networked environment.
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	Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans

TERM	DEFINITION
	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 Sniffing	Also referred to as "packet sniffing" or "sniffing." A technique that passively monitors or collects network communications, decodes protocols, and examines contents for information of interest.
NIST	National Institute of Standards and Technology
NMAP	Security-scanning software that maps networks and identifies open ports in network resources
Non-Console Access	Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.
Non-Consumer 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.
NVD	Acronym for "National Vulnerability Database." The U.S. government repository of standards-based vulnerability management data. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
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.

TERM	DEFINITION
	OWASP maintains a list of critical vulnerabilities for web applications. (See OWASP).
PAN	Acronym for "primary account number" and 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.
Password / Passphrase	A string of characters that serve as an authenticator of the user.
Patch	Update to existing software to add functionality or to correct a defect
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties
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.
Payment Processor	Sometimes referred to as "payment gateway" or "payment service provider (PSP)". Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
PCI	Acronym for "Payment Card Industry."
PCICC	Acronym for "Payment Card Industry Compliance Committee." Consists of campus specialized personnel from division of Information Technology, Administration & Finance, ASC, ASI & Philanthropic.
PCI DSS	Acronym for "Payment Card Industry Data Security Standard."
Penetration Test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs

TERM	DEFINITION
	from both outside the environment (external testing) and from inside the environment.
Personal Firewall Software	Information that can be utilized to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, 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	Acronym for "personal identification number." 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.
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
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POP3	Acronym for "Post Office Protocol v3." Application-layer protocol used by email clients to retrieve e-mail from a remote server over a TCP/IP connection.
Port	Logical (virtual) connection points associated with a particular communication protocol to facilitate communications across networks.

TERM	DEFINITION
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
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. See also Public Network
Privileged User	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.
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.
Proxy Server	A server that acts as an intermediary between an internal network and the Internet. For example, one function of a proxy server is to terminate or negotiate connections between internal and external connections such that each only communicates with the proxy server.
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 PCI Security Standards.
Public Network	Network established and operated by a third party telecommunications provider for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to, the Internet, wireless, and mobile technologies. See also Private Network

TERM	DEFINITION
QIR	Acronym for "Qualified Integrator or Reseller." Refer to the QIR Program Guide on the PCI SSC website for more information.
QSA	Acronym for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.
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 from a location outside of that network. Remote access connections can originate either from inside the company's own network or from a remote location outside the company's network. An example of technology for remote access is VPN
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 external/portable hard drives
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
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.
Risk Ranking	A defined criterion of measurement based upon the risk assessment and risk analysis performed on a given entity
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

TERM	DEFINITION
	information to proper destinations. Software routers are sometimes referred to as gateways.
S-FTP	Acronym for Secure-FTP. S-FTP has the ability to encrypt authentication information and data files in transit. See FTP
SAD	Sensitive Authentication Data
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 SANS website.)
SAQ	Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment
Schema	Formal description of how a database is constructed including the organization of data elements.
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" or "software development lifecycle." 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 Cryptographic Device	A set of hardware, software and firmware that implements cryptographic processes (including cryptographic algorithms and key generation) and is contained within a defined cryptographic boundary. Examples of secure cryptographic devices include host/hardware security modules (HSMs)

TERM	DEFINITION
	and point-of-interaction devices (POIs) that have been validated to PCI PTS.
Secure Wipe	Also called "secure delete," a method of overwriting data residing on a hard disk drive or other digital media, rendering the data irretrievable.
Security Event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.
Security Officer	Primary person responsible for an entity's security-related matters.
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, HTTPS, etc.
Sensitive Area	Any data center, server room or any area that houses systems that store, process, or transmit 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 track data (from the magnetic stripe or equivalent on a chip), 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

TERM	DEFINITION
	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 on behalf of another entity. 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. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
Session Token	In the context of web session management, a session token (also referred to as a "session identifier" or "session ID"), is a unique identifier (such as a "cookie") used to track a particular session between a web browser and a webserver.
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	A method by 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.

TERM	DEFINITION
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." Industry standard that encrypts the channel between a web browser and web server. Now superseded by TLS. See TLS.
Stateful Inspection	Also called "dynamic packet filtering." Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected.
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is "one way"; that is, not reversible). See Hashing. At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (Computer Security Resource Center Publications) for more guidance on cryptographic key strengths and algorithms.

TERM	DEFINITION
	Note: The above examples are appropriate for persistent storage of cardholder data. The minimum cryptography requirements for transaction- based operations, as defined in PCI PIN and PTS, are more flexible as there are additional controls in place to reduce the level of exposure. It is recommended that all new implementations use a minimum of 128-bits of effective key strength.
SysAdmin	Abbreviation for "system administrator." Individual with elevated privileges who is responsible for managing a computer system or network.
System Components	Any network devices, servers, computing devices, or applications 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 database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and 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 multi-factor authentication.
TCP	Acronym for "Transmission Control Protocol." One of the core transport-layer protocols of the Internet Protocol (IP) suite, and the basic communication language or protocol of the Internet. See IP.
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.

TERM	DEFINITION
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 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	In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or multi-factor authentication. See RADIUS, TACACS, and VPN. See also Session Token.
Track Data	Also referred to as "full track data" or "magnetic-stripe 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.
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.

TERM	DEFINITION
Untrusted Network	Network that is external to the networks belonging to an organization and which is out of the organization's ability to control or manage.
URL	Acronym for "Uniform Resource Locator." A formatted text string used by Web browsers, e-mail clients, and other software to identify a network resource on the Internet.
Versioning Methodology	A process of assigning version schemes to uniquely identify a particular state of an application or software. These schemes follow a version-number format, version-number usage, and any wildcard element as defined by the software vendor. Version numbers are generally assigned in increasing order and correspond to a particular change in the software.
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 Payment Terminal	A virtual payment 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 payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

TERM	DEFINITION
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.
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.
VPN	Acronym for “virtual private network.” A computer network in which some of 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.
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.

TERM	DEFINITION
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.
Wildcard	A character that may be substituted for a defined subset of possible characters in an application version scheme. In the context of PA-DSS, wildcards can optionally be used to represent a non-security impacting change. A wildcard is the only variable element of the vendor's version scheme, and is used to indicate there are only minor, non-security-impacting changes between each version represented by the wildcard element.
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.

REVISION CONTROL

Last Revised: 7/6/2020

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
Draft	6/27/2017	Tony Modiri/Lydia Rodriguez	Created the draft	All
1.1	10/31/2017	Tony Modiri/Lydia Rodriguez	Reviewed and updated	All
1.2	11/1/2017	Tony Modiri/Lydia Rodriguez	Reviewed and updated	Added Appendices
1.3	10/23/2018	Tony Modiri	Reviewed and updated	Section V.C
1.4	1/16/2019	Tony Modiri/Rachal Lasser	Reviewed	All
1.4.1	7/6/2020	Tony Modiri	Added Revision Control	Added Revision Control
1.4.2	7/29/2021	Bill Elbettar	Fix and update web links	DEFINITIONS, IMPLEMENTATION & ACCOUNTABILITY

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
11/1/2017	Tony Modiri	Approved
10/23/2018	Tony Modiri	Approved
7/6/2020	Tony Modiri	Approved
7/29/2021	Bill Elbettar	Approved