PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) INFORMATION SECURITY PROGRAM

The University of Texas at El Paso

TABLE OF CONTENTS

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) Program provides definitive information on the prescribed measures used to establish and enforce the Information Security Program for PCI DSS v3.2 compliance at The University of Texas at El Paso ("UTEP", also referred to as the "University" or "Institution").

UTEP is committed to protecting its employees, partners, clients and UTEP from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every UTEP user who interacts with data and Information Resources (IR). Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

Protecting University information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of Information Resources must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of cardholder data and Information Resources. This also includes against accidental loss or destruction.

PURPOSE

The purpose of the PCI DSS Information Security Policy is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of UTEP's payment card data and related Information Resources.
- Protecting UTEP, its employees, and its clients from illicit use of UTEP's Information Resources.
- Ensuring the effectiveness of security controls over data and Information Resources that support UTEP's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective University-wide management and oversight of those related Information Security risks.

The formation of the policy is driven by many factors, with the key factor being risk. This policy sets the ground rules under which UTEP shall operate and safeguard its data and Information Resources to both reduce risk and minimize the effect of potential incidents.

This policy, including related standards and procedures, are necessary to support the management of information risks in daily operations. The development of policy provides due care to ensure UTEP users understand their day-to-day security responsibilities and the threats that could impact the University.

Implementing consistent security controls across the Institution will help UTEP comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity and availability of UTEP data.

SCOPE & APPLICABILITY

This policy and its related standards, procedures, and guidelines apply to all UTEP data, Information Resources, activities, and assets owned, leased, controlled, or used by UTEP, its agents, contractors, or other business partners on behalf of UTEP that are within scope of the PCI DSS. This policy applies to all UTEP employees, contractors, sub-contractors, and their respective facilities supporting UTEP business operations, wherever UTEP data is stored or processed, including any third-party contracted by UTEP to handle, process, transmit, store, or dispose of UTEP data.

Some standards are explicitly stated for persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting UTEP business functions shall comply with the standards. UTEP departments shall use this policy and its standards or may create a more restrictive set of policies and standards, but not one that is less restrictive, less comprehensive, or less compliant than this policy and its standards.

This policy and its standards do not supersede any other applicable law or higher-level Institutional directive in effect as of the effective date of this policy.

Appendix D: Information Security Roles & Responsibilities provides a detailed description of UTEP user roles and responsibilities, in regards to Information Security.

UTEP reserves the right to revoke, change, or supplement this policy and its standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately unless otherwise stated. It is important to note that not ALL sections of this policy apply to all SAQs alike. This policy is based on the highest level of PCI DSS compliance. For specific requirements (i.e., sections of this document) that apply based on a specific SAQ level, please refer to the PCI DSS Document Library, SAQs

POLICY

UTEP shall design, implement and maintain a coherent set of standards and procedures to manage risks to cardholder data, in an effort to ensure an acceptable level of Information Security risk. Within the scope of the Cardholder Data Environment (CDE), UTEP will protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its Information Resources and cardholder data, regardless of how it is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

VIOLATIONS

Any UTEP user found to have violated any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution. UTEP Standard 24: Disciplinary Actions applies as well.

EXCEPTIONS

While every exception to a policy or standard potentially weakens protection mechanisms for UTEP Information Resources and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in Appendix E: Information Security Exception Request Procedures.

UPDATES

Updates to the PCI DSS Information Security Policy will be announced to employees via University updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, standards, procedures, and guidelines.

KEY TERMINOLOGY

In the realm of information security terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the primary reference document that UTEP uses to define common information security terms. [1] Please refer to the Definitions section of the UTEP Information Resources Use and Security Policy for additional information. Key terminology to be aware of includes:

Data Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Contract Owner: A term describing a person or entity that has been given formal responsibility for entering into and managing legal contracts with service providers. Contract owners are formally responsible for making sure due care and due diligence is performed with service providers, in regards to PCI DSS compliance.

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help UTEP accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized best practice to align UTEP with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. Appendix A: Data Classification & Handling Guidelines provides guidance on data classification and handling restrictions.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Data owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized best practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System: A term describing an asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

[1] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the data custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include Personally Identifiable Information, Payment Card Data (PCD), and all other forms of data classified as Confidential or Controlled in Appendix A: Data Classification & Handling Guidelines.

Service Provider: A term that 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 a company provides a service that involves only the provision of public network access (such as a telecommunications company providing just the communication link) that entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Sensitive Personally Identifiable Information (sPII): sPII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: [2]

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or other government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Standard: A term describing formally established requirements in regard to processes, actions, and configurations.

[2] The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - http://www.leg.state.or.us/ors/646a.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

INFORMATION SECURITY CONSIDERATIONS FOR PROTECTING SYSTEMS

Appendix F: Type of Security Controls provides a detailed description of information security considerations in protecting Information Resources, based on the importance of the system and the sensitivity of the data processed or stored by the system.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Information security documentation is comprised of four main parts: a core policy; measureable standards used to quantify the policy; procedures that must be followed; and guidelines that are recommended, but not mandatory.

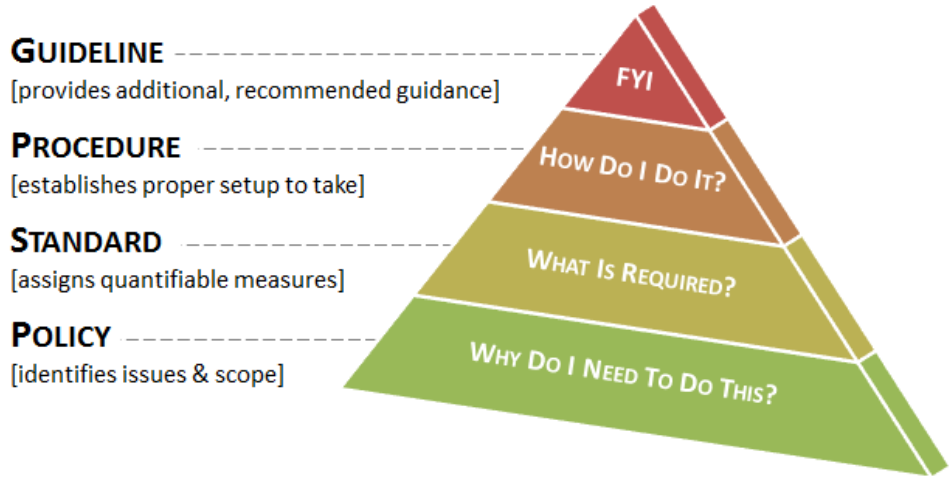


Figure 1: Policy Framework

INFORMATION SECURITY CONTROLS

Security controls are sometimes synonymous with standards, since controls are generally designed to directly map to standards. The PCI DSS Information Security Policy security controls have a well-defined organization and structure, which supports ongoing compliance with the PCI DSS.

INFORMATION SECURITY PROGRAM ACTIVITIES

An Information Security Management System (ISMS) focuses on information security management and IT-related risks. The governing principle behind UTEP's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with ISO/IEC 27001, UTEP's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This has involves making changes, where necessary, to bring the ISMS back to optimal performance.

REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between UTEP's networks and untrusted networks, as well as traffic into and out of more sensitive areas within UTEP's internal trusted networks. The Cardholder Data Environment (CDE) is an example of a more sensitive area within UTEP's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in PCI DSS Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of PCI DSS Requirement 1.

PCI DSS CONTROL 1.1

Control Intent: The organization establishes firewall and router configuration standards that follow industry-recognized best practices.

Standard: Data custodians are required to establish firewall and router configuration processes that include the following: [3]

(a) Data custodians are required to establish and maintaining a formal process for approving and testing all network connections and changes to both firewall and router configurations; [4]

(b) Data custodians are required to establish and maintaining detailed network diagrams. Network diagrams must: [5]
   1. Document all connections to cardholder data, including any wireless networks;
   2. Be reviewed annually; and
   3. Be updated as the network changes to reflect the current architecture in place;

(c) Data custodians are required to establish and maintaining detailed data flow diagrams that shows all cardholder data flows across systems and networks; A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and UTEP's internal networks; [6]

(d) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes; [7]

(e) A documented business justification is required for all services, protocols, and ports allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure; [8] and

(f) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover: [9]
   1. Validation of Access Control Lists (ACLs); and
   2. Vulnerability management (e.g., validating software and firmware is current).

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP)

[3] PCI DSS version 3.2 Requirement 1.1
[4] PCI DSS version 3.2 Requirement 1.1.1
[5] PCI DSS version 3.2 Requirement 1.1.2
[6] PCI DSS version 3.2 Requirement 1.1.4
[7] PCI DSS version 3.2 Requirement 1.1.5
[8] PCI DSS version 3.2 Requirement 1.1.6
[9] PCI DSS version 3.2 Requirement 1.1.7

Procedure for Requesting Static IP, DNS entries, and Firewall Changes

In an effort to mitigate the potential for servers being compromised due to misconfigurations or insecure settings, all requests for static IP's, DNS entries, or firewall changes must route through the Information Security Office (ISO) for approval. The ISO reviews server security when these items are requested to help minimize the attack surface that these servers may present.

- When requesting a static IP, DNS entry, or firewall change, a Service Desk request will need to be created and assigned to the Telecommunications Infrastructure (TI, aka Networking) Team. The request should include the following information if applicable :
    - Will this site or system store, gather, process, or access confidential data (some examples include but are not limited to):
        - Username/passwords
        - Research data
        - SSNs
        - UTEP ID
        - Student Educational Records
        - Financial Info (Bank Routing, etc.)
        - Credit Card info
        - Etc.

  For more information please refer to UTEP Standard 9: Data Classification and Extended List of Confidential Data.

- TI will send an approval request through the service desk application to the ISO for review and scanning.

- If your request is for a website, is it "production ready"; if so, can the ISO perform a vulnerability scan? A report will be sent by email with the results of the scan. If the server is not currently up and running, the ISO will provisionally provide the static IP so that the system can be built up, however it will still be required to pass the vulnerability scan once the system is production ready. Please note that the report is interactive and clicking on any listed vulnerability will provide additional information with more information and suggestions for resolving the issue.

- The ISO highly recommends that a back-up be performed on the server as there may be a slight chance that the scan may cause an issue or crash the server. This may include a backup of any configuration files, and other important data that may reside on the system.

- If the vulnerability scan flags any issues, they will need to be addressed first. The Service Desk request will be assigned to the ISO until all issues are resolved.

- Once the flagged issues are resolved and the request is approved by the ISO, it will be routed to the appropriate group in IT so that the request can be completed.

- If your system has not been scanned in over a month, it will need to be scanned again for any new changes to the firewall or DNS entries.

PCI DSS CONTROL 1.2

Control Intent: The University builds firewall and router configurations that restrict connections between untrusted networks and any system components in the Cardholder Data Environment (CDE).

Standard: Data custodians are required to ensure that firewall and router deployment and configuration restrict connections between untrusted networks and any system components within the Cardholder Data Environment (CDE) by the following means: [10]

(a) Implementing Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to the CDE to only that which is necessary, as defined by a business justification; [11]
(b) Securing and synchronizing router and firewall configuration files; [12] and

[10] PCI DSS version 3.2 Requirement 1.2
[11] PCI DSS version 3.2 Requirement 1.2.1
[12] PCI DSS version 3.2 Requirement 1.2.2

(c) Positioning perimeter firewalls between wireless networks and the CDE.[13]

Supplemental Guidance: Not all firewalls and routers have the functionality for the running configuration to be different that the configuration loaded at startup. However, if the functionality exists, the startup configuration must be synchronized with the correct running configuration so that a reboot of the device will not degrade network security.

Please refer to the UTEP Standard 19: Server and Device Configuration and Management

PCI DSS CONTROL 1.3

Control Intent: The University prohibits direct public access between the Internet and any system component in the Cardholder Data Environment (CDE).

Standard: Data custodians are responsible for ensuring that firewall and router configuration standards are established and managed to prohibit direct public access between the Internet and any system component in the Cardholder Data Environment (CDE) that includes, but is not limited to: [14]

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [15]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [16]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [17]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [18]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [19]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [20] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [21]

Supplemental Guidance: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated, so that filtering decisions would not only be based on administrator-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection.

Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT),
- Placing servers containing cardholder data behind proxy servers/firewalls,
- Removal or filtering of route advertisements for private networks that employ registered addressing, or
- Internal use of RFC1918 address space instead of registered addresses.

Please refer to Control 1.1 above: Procedure for Requesting Static IP, DNS entries, and Firewall Changes

PCI DSS CONTROL 1.4

Control Intent: The University requires that a personal firewall software be installed and/or enabled on any mobile and/or employee-owned computers accessing the Card Holder Data Environment (CDE) and with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the University's network.

Standard: Data custodians are required to install and maintain firewall software, or equivalent functionality, on any Internet-accessible mobile device or computer which are used to access the CDE that includes, but is not limited to: [22]

[13] PCI DSS version 3.2 Requirement 1.2.3
[14] PCI DSS version 3.2 Requirement 1.3
[15] PCI DSS version 3.2 Requirement 1.3.1
[16] PCI DSS version 3.2 Requirement 1.3.2
[17] PCI DSS version 3.2 Requirement 1.3.3
[18] PCI DSS version 3.2 Requirement 1.3.4
[19] PCI DSS version 3.2 Requirement 1.3.5
[20] PCI DSS version 3.2 Requirement 1.3.6
[21] PCI DSS version 3.2 Requirement 1.3.7
[22] PCI DSS version 3.2 Requirement 1.4

(a) Firewall software must be audited by the ISO;
(b) Configuration settings of the firewall software must not be alterable by standard users; and
(c) Firewall configurations must include:
    1. Specific configuration settings are defined for firewall software.
    2. Firewall software is actively running.
    3. Firewall software is not alterable by users of mobile devices and/or computers.

Supplemental Guidance: Examples of mobile devices and computers includes, but are not limited to:

- Laptops
- Tablets
- Smart phones

Please refer to the UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 8: Malware Prevention; UTEP Standard 11: Safeguarding Data; UTEP Standard 19: Server and Device Configuration and Management; and UTEP Minimum Security Standards for Systems.

PCI DSS CONTROL 1.5

Control Intent: Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for managing firewalls are kept current and disseminated to all pertinent parties. [23]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Please refer to Control 1.1 above: Procedure for Requesting Static IP, DNS entries, and Firewall Changes

[23] PCI DSS version 3.2 Requirement 1.5

REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS

Malicious individuals (external and internal to an institution) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS CONTROL 2.1

Control Intent: The University always changes vendor-supplied defaults before installing a system on the network.

Standard: Data custodians are required to ensure vendor-supplied defaults are changed, prior to the information system being installed on the network. This pre-production hardening process for both wired and wireless information systems must include, but is not limited to: [24]

(a) Changing vendor default credentials: [25]
    1. Passwords;
    2. Simple Network Management Protocol (SNMP) community strings; and
    3. Encryption keys
(b) Disabling or deleting unnecessary accounts;
(c) Updating firmware on devices; and
(d) Verifying other security-related vendor defaults are changed, if applicable.

Supplemental Guidance: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc. Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.

Please refer to the UTEP Standard 4: Access Management; UTEP Standard 19: Server and Device Configuration and Management; and UTEP System Hardening, Web Application Guides and Hosted IT Services Checklist

PCI DSS CONTROL 2.2

Control Intent: The University develops configuration standards for all system components that are consistent with industry-accepted system hardening standards.

Standard: Data custodians are required to develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to: [26]

(a) Verifying that system configuration standards are:
    1. Updated as new vulnerability issues are identified;
    2. Applied when new systems are configured;
    3. Consistent with industry-accepted hardening standards;
(b) Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers); [27]
(c) Enforcing least functionality, which includes but is not limited to:
    1. Allowing only necessary and secure services, protocols, and daemons; [28]
    2. Removing all unnecessary functionality, which includes but is not limited to: [29]
        i. Scripts;
        ii. Drivers;
        iii. Features;
        iv. Subsystems;
        v. File systems; and
        vi. Unnecessary web servers

[24] PCI DSS version 3.2 Requirement 2.1
[25] PCI DSS version 3.2 Requirement 2.1.1
[26] PCI DSS version 3.2 Requirement 2.2
[27] PCI DSS version 3.2 Requirement 2.2.1
[28] PCI DSS version 3.2 Requirement 2.2.2
[29] PCI DSS version 3.2 Requirement 2.2.5

(d) Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP; [30]
(e) Verifying system security parameters are configured to prevent misuse; [31] and
(f) Documenting the functionality present on Information Resources.

Supplemental Guidance: Appendix J: System Hardening contains the approved baseline configurations. Baseline configurations should be based on industry-recognized best practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs) [32]
- UTEP Windows 10 Standalone Configuration

If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

Please refer to the UTEP Standard 4: Access Management; UTEP Standard 19: Server and Device Configuration and Management; and UTEP System Hardening, Web Application Guides and Hosted IT Services Checklist

PCI DSS CONTROL 2.3

Control Intent: The University encrypts all non-console administrative access using strong cryptography.

Standard: Data custodians are responsible for developing configuration standards to ensure all non-console administrative access is encrypted using strong cryptography using technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. [33]

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP);
- Telnet; and
- Post Office Protocol 3 (POP3).

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 4: Access Management (4.3b) ; UTEP Standard 11: Safeguarding Data; and UTEP Standard 19: Server and Device Configuration and Management. UTEP Data Encryption Guidelines

PCI DSS CONTROL 2.4

Control Intent: The University maintains an inventory of system components that are in scope for PCI DSS.

Standard: Data custodians are required to maintain an inventory of UTEP's Information Resources that are in scope for PCI DSS and update the inventory as necessary. [34]

Supplemental Guidance: Maintaining a current list of all system components will enable the University to accurately and efficiently define the scope of its CDE for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from applicable configuration standards.

The data custodian shall submit a PCI System Registration Information form for any system that is in scope for PCI DSS to the ISO. Likewise, if a system falls out of scope the ISO will be notified via email. Data custodian are responsible for updating the inventory list and providing the ISO with a registration form anytime a new system falls in scope for PCI DSS. The form is provided below:

[30] PCI DSS version 3.2 Requirement 2.2.3
[31] PCI DSS version 3.2 Requirement 2.2.4
[32] DISA STIGs official site: http://iase.disa.mil/stigs/index.html
[33] PCI DSS version 3.2 Requirement 2.3
[34] PCI DSS version 3.2 Requirement 2.4

PCI System Registration Information

The University of Texas at El Paso

Information Security Office

INFORMATION RESOURCE OWNER	
DATE:	Click here to enter text.
DEPARTMENT HEAD:	Click here to enter text.
MERCHANT REPRESENTATIVE:	Click here to enter text.
DEPARTMENT:	Click here to enter text.
PHONE NUMBER:	Click here to enter text.
BUILDING & ROOM NUMBER:	Click here to enter text.
Device Information	
DEVICE TYPE:	Click here to enter text.
MAC ADDRES:	Click here to enter text.
IP ADDRESS:	Click here to enter text.
UTEP TAG# OR SERIAL#:	Click here to enter text.
DEVICE NETWORK NAME:	Click here to enter text.
DEVICE LOCATION:	Click here to enter text.
MERCHANT CUSTODIAN/SYSADM:	Click here to enter text.
EXTENSION:	Click here to enter text.
DEPARTMENT:	Click here to enter text.
BLDG/ROOM:	Click here to enter text.
EMAIL:	Click here to enter text.
Data Classification	☐ **CONFIDENTIAL** ☐ **CONTROLLED** ☐ **PUBLISHED**

Please describe the system's main function:
Click here to enter text.

PCI DSS CONTROL 2.5

Control Intent: The University ensures that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for managing vendor defaults and other security parameters are kept current and disseminated to all pertinent parties. [35]

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 4: Access Management; UTEP Standard 5: Administrative/Special Access Accounts; UTEP Standard 10: Risk Management; UTEP Standard 11: Safeguarding Data; UTEP

[35] PCI DSS version 3.2 Requirement 2.5

Standard 16: Data Center Security; UTEP Standard 19: Server and Device Configuration and Management; UTEP Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance

PCI DSS CONTROL 2.6

Control Intent: The University's shared hosting providers protect the University's hosted environment and cardholder data.

Standard: For shared hosting providers, UTEP's contract owners, data custodians and data owners are required to: [36]

(a) Maintain a comprehensive list of those service providers, including all applicable Service Level Agreements (SLAs);
(b) Require that providers of external information systems comply with UTEP information security requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements (e.g., PCI DSS);
(c) Define oversight responsibilities with regard to external information system services;
(d) Perform a review of the service provided for acceptable service levels;
(e) Conduct a risk assessment outsourcing of services; and
(f) Monitor security control compliance by those external service providers.

Supplemental Guidance: These providers must meet specific requirements as detailed in Appendix A (Additional PCI DSS Requirements for Shared Hosting Provider) of the PCI DSS. Additionally, a "Request for Vendor User Account Approval" form (below) must be submitted to request access to UTEP Cardholder Data Environment and/or information resources.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 4: Access Management; UTEP Standard 5: Administrative/Special Access Accounts; UTEP Standard 10: Risk Management; UTEP Standard 11: Safeguarding Data; UTEP Standard 16: Data Center Security; UTEP Standard 19: Server and Device Configuration and Management; UTEP Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance

[36] PCI DSS version 3.2 Requirement 2.6

Information Security Office PCI DSS

Vendor User Account Approval Form

Applicant Section

I understand that the access being granted through my administrative office staff account is assigned to me at the request of the Department Head. It is to be used only in connection with my assigned duties as a vendor, consultant, or otherwise an employee of UTEP and may be revoked without notice upon the request of the administrator. I understand and accept the following terms and conditions:

- I agree not to reveal my password nor allow anyone to use the account assigned to me. I am responsible for any changes made under my credentials.
- I agree to abide by the Payment Card Industry Data Security Standard (PCI DSS), as well as The University of Texas at El Paso PCI DSS Policy, and the Acceptable Use Agreement.
- I agree to maintain the security of customer information, including payment cardholder information such as payment card number, payment cardholder name, expiration date, and payment cardholder verification number. I agree to refer *all outside requests* for cardholder information to the Information Security Office.
- I agree to maintain the confidentiality of any and all data that I retrieve in the course of my duties, including data that I use for reporting purposes or in other software products.
- I agree that it is my responsibility to prevent unauthorized access and disclosure of the data within my possession.
- Access to administrative data will be determined by the requirements of my vendor agreement, and therefore I am only authorized to retrieve this data on a "need to know" basis.
- I agree to comply with all UTEP policies including but not limited to Information Security policies, University of Texas System policies, computer access standards, confidentiality of data standards, data entry standards, and data integrity standards.

I am aware that any violation of these policies or standards may lead to the immediate suspension of my computer privileges. I understand that unauthorized release of sensitive or restricted information is a breach of data security and may be cause for disciplinary action, up to and including termination of agreement, and may be subject to or include civil and criminal prosecution.

Applicant Information:

Signature: _____ Date: _____

Name: _____ Email: _____

Job Title: _____ Company: _____

Phone: _____ Bldg/Room: _____

Address:

Job Function or Special Instructions:

_____

_____

Department Head: I authorize a user id or the changes listed for the above person. I understand that it is my responsibility to make appropriate changes when there is a change in the applicant's status.

Dept. Head Signature: _____ Date: _____

Dept. Head Name (Please Print): _____

Please Fax this form to (915) 747-5250 or E-Mail to security@utep.edu

Approval: _____ Date: _____

Chief Information Security Officer

REQUIREMENT #3: PROTECT STORED CARDHOLDER DATA

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

PCI DSS CONTROL 3.1

Control Intent: The University implements a process to minimize the storage of cardholder data.

Standard: Data owners are required to determine the business requirements for data retention and securely dispose of cardholder data once the data is no longer necessary. This includes, but is not limited to: [37]

(a) Implement a data retention and disposal policy that covers cardholder data;
(b) Limiting cardholder data retention time to that which is required for legal, regulatory, and business requirements;
(c) Conducting a quarterly process (automatic or manual) to identify and securely delete stored cardholder data that exceeds defined retention requirements.
(d) Performing secure deletion of electronic-based cardholder data; and
(e) Shredding physical-based cardholder data.

Supplemental Guidance: Specific requirements for the retention of cardholder data are driven by business needs (e.g., cardholder data needs to be held for X period for Y business reasons) and documentation should exist to justify the business need.

Please refer to the UTEP Purchasing & General Services Records Management website: http://admin.utep.edu/Default.aspx?tabid=1677. Additional information may be found here: UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 9: Data Classification; and UTEP Standard 11: Safeguarding Data;

PCI DSS CONTROL 3.2

Control Intent: The University does not store sensitive authentication data after authorization.

Standard: Data custodians are required to ensure sensitive authentication data is not stored after authorization, even if it is encrypted. UTEP is prohibited from storing: [38]

(a) The full contents of any track: [39]
    1. Tracks are from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere.
    2. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
(b) Storing the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions; [40] and
(c) Storing the Personal Identification Number (PIN) or the encrypted PIN block. [41]

Supplemental Guidance: The following data sources should be examined to verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance:

- Incoming transaction data;
- All logs (e.g., transaction, history, debugging, error);
- History files;
- Trace files;
- Several database schemas; and
- Database contents.

[37] PCI DSS version 3.2 Requirement 3.1
[38] PCI DSS version 3.2 Requirement 3.2
[39] PCI DSS version 3.2 Requirement 3.2.1
[40] PCI DSS version 3.2 Requirement 3.2.2
[41] PCI DSS version 3.2 Requirement 3.2.3

PCI DSS CONTROL 3.3

Control Intent: The University masks the Primary Account Number (PAN) when displayed.

Standard: Data owners, in conjunction with Data custodians, are required to ensure the PAN is masked so no more than the first six (6) and last four (4) digits are the maximum number of digits allowed to be displayed and/or printed.[42]

Supplemental Guidance: Only users with a legitimate business need to see the full PAN are allowed an exception to this requirement.

Credit card devices are fully compliant with this control and mask the PAN so that no more than the first six and last four digits are displayed/printed. Please refer to UTEP Standard 23: Security Control Exceptions; and Appendix E: Information Security Exception Request Procedures

PCI DSS CONTROL 3.4

Control Intent: The University implements a process to ensure Primary Account Numbers (PANs) are rendered unreadable anywhere PANs are stored.

Standard: Data custodians, in conjunction with data owners, are required to implement technical measures to ensure PANs are not accessible by unauthorized users or processes by using any of the following approaches: [43]

(a) Render PANs unreadable anywhere PANs are stored, including on portable digital media, backup media, and in logs through the means of:
    1. One-way hashes based on strong cryptography (hash must be of the entire PAN);
    2. Truncation (hashing cannot be used to replace the truncated segment of PAN);
    3. Index tokens and pads (pads must be securely stored); or
    4. Strong cryptography with associated key-management processes and procedures; and
(b) Preventing decryption keys from being tied to user accounts, if disk encryption is used, rather than file- or column-level database encryption: [44]
    1. Logical access must be managed independently of native operating system access control mechanisms (e.g., by not using local user account databases).
    2. Decryption keys must not be tied to operating system-level user accounts.

Supplemental Guidance: Since it is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN, where hashed and truncated versions of the same PAN are present in UTEP's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

Please refer to The UTEP Payment Card Industry Cryptographic Keys document.

PCI DSS CONTROL 3.5

Control Intent: The University implements a key management strategy to protect keys used to secure cardholder data against disclosure and misuse.

Standard: Data owners are required to implement administrative and technical measures to protect keys used to secure cardholder data against disclosure and misuse, including the following: [45]

(a) Maintain a documented description of the cryptographic architecture that includes: [46]
    1. Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date;
    2. Description of the key usage for each key; and
    3. Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management;
(b) Cryptographic key access shall be restricted to the fewest number of custodians necessary; [47]
(c) Cryptographic key access shall be securely stored at all times using one of the following methods: [48]

[42] PCI DSS version 3.2 Requirement 3.3
[43] PCI DSS version 3.2 Requirement 3.4
[44] PCI DSS version 3.2 Requirement 3.4.1
[45] PCI DSS version 3.2 Requirement 3.5
[46] PCI DSS version 3.2 Requirement 3.5.1
[47] PCI DSS version 3.2 Requirement 3.5.2
[48] PCI DSS version 3.2 Requirement 3.5.3

1. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key;
2. Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device); or
3. As at least two full-length key components or key shares, in accordance with an industry-accepted method; and

(d) Cryptographic keys must be securely stored in the fewest possible locations and forms. [49]

Supplemental Guidance: This requirement also applies to key-encrypting keys used to protect data-encrypting keys. This requires that key-encrypting keys must be at least as strong as the data-encrypting key.

Please refer to The UTEP Payment Card Industry Cryptographic Keys document.

PCI DSS CONTROL 3.6

Control Intent: The University documents and implements key management processes and procedures for cryptographic keys used for encryption of cardholder data.

Standard: Data owners are required to document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data that includes the following: [50]

(a) Procedures for the generation, distribution and storage of keys:
   1. Generation of strong cryptographic keys; [51]
   2. Prevention of unauthorized substitution of cryptographic keys; [52]
   3. Distribution of cryptographic keys using secure methods; [53] and
   4. Secure storage of cryptographic keys; [54]

(b) Changing cryptographic keys that have reached the end of their cryptoperiod: [55]
   1. After a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key;
   2. As defined by the associated application vendor or key owner; or
   3. Based on industry best practices and guidelines (e.g., NIST Special Publication 800-57).

(c) Retiring or replacing keys when the integrity of the key has been weakened or the keys are suspected of being compromised: [56]
   1. Retiring or replacing may be performed by archiving, destruction, and/or revocation of keys.
   2. Keys should be considered compromised by departure of an employee with knowledge of a clear-text key.

(d) Split knowledge and dual control, if manual, clear-text cryptographic key management operations are used. If applicable, these operations require procedures that require two or three people, each knowing only their own key component, to reconstruct the whole key; [57] and

(e) Requiring cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. [58]

Supplemental Guidance: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.

Please refer to The UTEP Payment Card Industry Cryptographic Keys document. Additionally, please refer to UTEP Standard 11: Safeguarding Data, § 11.4 Assured Access to Encrypted Data

PCI DSS CONTROL 3.7

Control Intent: The University ensures that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

[49] PCI DSS version 3.2 Requirement 3.5.4
[50] PCI DSS version 3.2 Requirement 3.6
[51] PCI DSS version 3.2 Requirement 3.6.1
[52] PCI DSS version 3.2 Requirement 3.6.7
[53] PCI DSS version 3.2 Requirement 3.6.2
[54] PCI DSS version 3.2 Requirement 3.6.3
[55] PCI DSS version 3.2 Requirement 3.6.4
[56] PCI DSS version 3.2 Requirement 3.6.5
[57] PCI DSS version 3.2 Requirement 3.6.6
[58] PCI DSS version 3.2 Requirement 3.6.8

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for protecting stored cardholder data are kept current and disseminated to all pertinent parties. [59]

Supplemental Guidance: Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

Annual training is conducted when SAQs are renewed in addition to annual UTEP Institutional Compliance Training. Additionally, the Information Security Office maintains a webpage for PCI standards and related documentation; it may be found here: http://admin.utep.edu/Default.aspx?tabid=73861. UTEP Policies and Standards may be accessed here: http://admin.utep.edu/Default.aspx?tabid=63604.

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

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS CONTROL 4.1

Control Intent: The University uses strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

Standard: To safeguard sensitive cardholder data during transmission, data custodians are required to ensure the following: [60]

(a) Only trusted keys and certificates are accepted;
(b) Strong cryptography and security protocols are used to safeguard sensitive cardholder data during transmission over open, public networks. Examples of technologies that support this requirement include, but are not limited to:
    1. Trans Layer Security (TLS);
    2. IP Security (IPSEC);
    3. Secure Shell (SSH); and
    4. Secure File Transfer Protocol (SFTP) / File Transfer Protocol - Secure (FTP-S); and
(c) Wireless networks transmitting cardholder data or connected to the Cardholder Data Environment (CDE), use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. [61]

Supplemental Guidance: Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:

- The Internet;
- Wireless technologies;
- Global System for Mobile communications (GSM); and
- General Packet Radio Service (GPRS).

Point of Sale Devices all use built-in certificates for transmitting PCI data over the network; applications use industry-accepted protocols like TLS V1.2 or above to transmit any PCI data. WiFi network is currently not in scope and is not being used for PCI purposes. Please refer to UTEP Standard 2: Acceptable Use of Information Resources; UTEP Standard 4: Access Management; UTEP Standard 9: Data Classification; UTEP Standard 11: Safeguarding Data; UTEP Standard 19: Server and Device Configuration and Management; and UTEP Standard 22: Vendor and Third-Party Controls and Compliance .

PCI DSS CONTROL 4.2

Control Intent: The University prohibits the transmission of unprotected Primary Account Numbers (PANs) by end-user messaging technologies.

Standard: UTEP prohibits the transmissions of unprotected PANs by end-user messaging technologies. [62]

Supplemental Guidance: Examples of end-user messaging technologies include, but are not limited to:

- Electronic mail (e-mail);
- Instant messaging (IM);

[59] PCI DSS version 3.2 Requirement 3.7
[60] PCI DSS version 3.2 Requirement 4.1
[61] PCI DSS version 3.2 Requirement 4.1.1
[62] PCI DSS version 3.2 Requirement 4.2

- Chat; and
- Short Message Service (SMS)

Please refer to UTEP Standard 2: Acceptable Use of Information Resources under "Confidentiality & Security of Data"; and Standard 4: Access Management; Standard 9: Data Classification; Standard 11: Safeguarding Data; and Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 4.3

Control Intent: The University ensures that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for encrypting transmissions of cardholder data are kept current and disseminated to all pertinent parties.[63]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources under "Confidentiality & Security of Data"; Standard 4: Access Management; Standard 11: Safeguarding Data; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, users are required to complete Institutional Compliance training on an annual basis titled "Information Security and Protecting the Confidentiality of SSNs – UTS165"

[63] PCI DSS version 3.2 Requirement 4.3

REQUIREMENT #5: USE & REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

Malicious software, commonly referred to as "malware" (including viruses, worms, rootkits and Trojans) enters network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices. This can result in the exploitation of system vulnerabilities, so anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS CONTROL 5.1

Control Intent: The University deploys anti-malware software on systems commonly affected by malicious software.

Standard: Data custodians are required to:

(a) Deploy the UTEP-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to: [64]
    1. Workstations;
    2. Servers;
    3. Tablets;
    4. Mobile phones;
(b) Ensure that the UTEP-approved anti-malware software is capable of detecting, removing, and protecting against all known types of malware; [65] and
(c) Perform periodic evaluations to identify and evaluate evolving malware threats on information systems considered to be not commonly affected by malware, in order to confirm whether such information systems continue to not require anti-malware software. [66]

Supplemental Guidance: Systems not capable of running anti-malware software should have a documented business justification as to why anti-malware software cannot be run and what compensating controls are in place to minimize the risk associated with the lack of anti-malware software on that system.

Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for institutions to be aware of new malware that might affect their systems. For example, by monitoring vendor security notices and anti-malware news groups to determine whether their systems might be coming under threat from new and evolving malware.

Trends in malware should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into UTEP's configuration standards and protection mechanisms as needed

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Account Management (4.3e); Standard 8: Malware Prevention; Standard 19: Server and Device Configuration and Management; Standard 20: Software Licensing (20.2); and Standard 23: Security Control Exceptions. Additionally please refer to the Security Exception Reporting Process.

PCI DSS CONTROL 5.2

Control Intent: The University ensures that anti-malware mechanisms are current, actively running, and generating audit logs.

Standard: Data custodians are required to ensure the UTEP-approved anti-malware software is: [67]

(a) Kept current with updates from the anti-malware vendor;
(b) Actively running on systems the anti-malware software is deployed to; and
(c) Generating audit logs per PCI DSS requirement 10.7.

Supplemental Guidance: Even the best anti-malware solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and

[64] PCI DSS version 3.2 Requirement 5.1
[65] PCI DSS version 3.2 Requirement 5.1.1
[66] PCI DSS version 3.2 Requirement 5.1.2
[67] PCI DSS version 3.2 Requirement 5.2

malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

Anti-malware test files from the European Institute for Computer Antivirus Research (EICAR) may be downloaded (http://www.eicar.org/85-0-Download.html) and copied to either a CD/DVD or write-protected USB.

- This CD/DVD or USB should be inserted into systems to test that anti-malware software is running "on demand" scans and detects the presence of the EICAR test file; and
- Logs should be checked to verify the EICAR test file was detected and logged.

PCI DSS CONTROL 5.3

Control Intent: The University ensures that anti-malware mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by the CISO on a case-by-case basis for a limited time period. Submission of an Exception request for approval by the CISO is required and needs to state a business justification and/or compensating control to be implemented.

Standard: Data custodians are required to ensure the UTEP-approved anti-malware software is actively running and cannot be disabled or altered by users, unless specifically authorized by the CISO on a case-by-case basis for a limited time period. Submission of an Exception request for approval by the CISO is required and needs to state a business justification and/or compensating control to be implemented.[68]

Supplemental Guidance: Anti-malware that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-malware protection is not active (e.g., disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled).

Anti-virus software must be installed and appropriately configured on all University-owned/leased systems. Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Account Management (4.3e); Standard 8: Malware Prevention; Standard 19: Server and Device Configuration and Management; and Standard 20: Software Licensing (20.2); and Standard 23: Security Control Exceptions. Additionally please refer to the Security Exception Reporting Process.

PCI DSS CONTROL 5.4

Control Intent: The University ensures that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.[69]

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for protecting systems against malware are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Account Management (4.3e); Standard 8: Malware Prevention; Standard 19: Server and Device Configuration and Management; Standard 20: Software Licensing (20.2); and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, users are required to complete Institutional Compliance training on an annual basis titled "Information Security and Protecting the Confidentiality of SSNs – UTS165".

[68] PCI DSS version 3.2 Requirement 5.3
[69] PCI DSS version 3.2 Requirement 5.4

REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & APPLICATIONS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Since many of these vulnerabilities are fixed by vendor-provided security patches, all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI DSS CONTROL 6.1

Control Intent: The University implements a process to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.

Standard: Data custodians and data owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system. [70]

Supplemental Guidance: The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.[71]

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Please refer to UTEP Standard 6: Backup and Disaster Recovery; Standard 7: Change Management; Standard 9: Data Classification; Standard 10: Risk Management; Standard 11: Safeguarding Data; and Standard 19: Server and Device Configuration and Management.

PCI DSS CONTROL 6.2

Control Intent: The University ensures that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

Standard: Data custodians and data owners are required to ensure that: [72]

(a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
(b) Critical security patches are installed within thirty (30) days of the vendor's release data; and
(c) Non-critical security patches are installed within ninety (90) days of the vendor's release data.

Supplemental Guidance: UTEP is allowed to apply a risk-based approach to prioritize its patch installations. For example, by prioritizing critical infrastructure (e.g., public-facing devices and systems, databases) higher than less-critical internal devices, this helps ensure high-priority systems and devices are addressed within one month and still allows for addressing less critical devices and systems within three months.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; and Standard 19: Server and Device Configuration Management. Additionally, the ISO reviews, tests, approves, and pushes Microsoft security patches on a monthly basis to all campus domain systems. The procedure includes downloading and applying patches on "Patch Tuesday" to ISO computers only. The patches are tested and if no issues are encountered they are then pushed to Information Technology systems on the Friday after patch Tuesday for broader testing. IT reports issues, if any are encountered, to ISO and the ISO determines whether the patch will be declined or pushed to the campus after further testing. Testing includes pushing updates to ISO servers prior to or on Maintenance Thursday (third Thursday of each month). A Bulletin is send out typically the Monday after patch Tuesday to all Faculty, Staff and Student Employees stating the date that Microsoft updates will be pushed to campus. If the patches do not cause issues they are pushed to all miner domain systems on the second Friday after "Patch Tuesday". This procedure occurs on a monthly basis. In addition, LINUX (all flavors) are installed on Production servers on the Wednesday and Thursday, aka Maintenance Night Thursday (3rd Thursday of the Month). Test environment (LINUX servers) are downloaded, installed and tested on Tuesday before Maintenance Night prior to releasing to Production on Wednesday and Thursday.

[70] PCI DSS version 3.2 Requirement 6.1
[71] National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm
[72] PCI DSS version 3.2 Requirement 6.2

PCI DSS CONTROL 6.3

Control Intent: The University develops all internal and external software applications in accordance with PCI DSS and based on industry best practices.

Standard: Contract owners, data custodians and data owners are required to ensure that internal and external developers:

(a) Develop software applications in accordance with PCI DSS and based on industry best practices; [73]
(b) Incorporate information security throughout the software development life cycle; [74]
(c) Remove custom application accounts, user IDs, and passwords before applications become active or are released to customers; [75] and
(d) Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: [76]
    1. Code changes must be reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices;
    2. Code reviews must ensure code is developed according to secure coding guidelines;
    3. Appropriate corrections must be implemented prior to release; and
    4. Code-review results must be reviewed and approved by management prior to release.

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[77]

Currently there are no developed applications in scope. Please refer to the UTEP Information Security Office Minimum Security Standards for Applications Development and Administration as well as UTEP Standard 7: Change Management.

PCI DSS CONTROL 6.4

Control Intent: The University follows change control processes and procedures for all changes to system components.

Standard: Data custodians and data owners are required to follow change control processes and procedures for all changes to system components. The change control processes for assets within scope for PCI DSS include the following: [78]

(a) Utilize separate environments for development/testing/staging and production; [79]
(b) Utilize a separation of duties between development/testing/staging and production environments; [80]
(c) Prohibit the use of production data (e.g., live PANs) for testing or development; [81]
(d) Remove test data and accounts before production systems become active / goes into production; [82] and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following: [83]
    1. Documentation of impact; [84]
    2. Documented change approval by authorized parties;[85]
    3. Functionality testing to verify that the change does not adversely impact the security of the system; [86] and
    4. Back-out procedures; [87] and
(f) Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. [88]

Supplemental Guidance: Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

---

[73] PCI DSS version 3.2 Requirement 6.3
[74] PCI DSS version 3.2 Requirement 6.3
[75] PCI DSS version 3.2 Requirement 6.3.1
[76] PCI DSS version 3.2 Requirement 6.3.2
[77] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[78] PCI DSS version 3.2 Requirement 6.4
[79] PCI DSS version 3.2 Requirement 6.4.1
[80] PCI DSS version 3.2 Requirement 6.4.2
[81] PCI DSS version 3.2 Requirement 6.4.3
[82] PCI DSS version 3.2 Requirement 6.4.4
[83] PCI DSS version 3.2 Requirement 6.4.5
[84] PCI DSS version 3.2 Requirement 6.4.5.1
[85] PCI DSS version 3.2 Requirement 6.4.5.2
[86] PCI DSS version 3.2 Requirement 6.4.5.3
[87] PCI DSS version 3.2 Requirement 6.4.5.4
[88] PCI DSS version 3.2 Requirement 6.4.6

Please refer to UTEP Standard 1: Information Resources Security Requirements and Accountability (1.14); Standard 4: Access Management (also 4.5-Data Access Control Requirements); UTEP Standard 6: Backup and Disaster Recovery; UTEP Standard 7: Configuration Management; UTEP Standard 19: Server and Device Configuration and Management; UTEP Standard 21: System Development and Deployment; and The University of Texas at El Paso Minimum Security Standards for Systems.

PCI DSS CONTROL 6.5

Control Intent: The University develops applications based on secure coding guidelines.

Standard: Contract owners, data custodians and data owners are required to address common coding vulnerabilities in the software-development process by ensuring the following:

(a) At least annually, developers are properly trained in current, secure coding techniques, including: [89]
    1. How to avoid common coding vulnerabilities, and
    2. Understanding how sensitive data is handled in memory

(b) Applications are developed based on secure coding guidelines: [90]
    1. Injection flaws, particularly SQL injection: [91]
        i. OS Command Injection;
        ii. LDAP and XPath injection flaws, and
        iii. Other forms of injection flaws;
    2. Buffer overflow; [92]
    3. Insecure cryptographic storage; [93]
    4. Insecure communications; [94]
    5. Improper error handling; [95]
    6. All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS requirement 6.1; [96]
    7. Cross-site scripting (XSS); [97]
    8. Improper access control, including but not limited to: [98]
        i. Insecure direct object references,
        ii. Failure to restrict URL access; and
        iii. Directory traversal;
    9. Cross-site request forgery (CSRF); [99] and
    10. Broken authentication and session management. [100]

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[101]

Currently there are no developed applications in scope. Please refer to the UTEP Information Security Office Minimum Security Standards for Applications Development and Administration as well as UTEP Standard 7: Change Management.

PCI DSS CONTROL 6.6

Control Intent: The University address new threats and vulnerabilities on an ongoing basis and ensure public-facing web applications are protected against known attacks.

Standard: Data custodians and data owners are required to address public-facing web application threats and vulnerabilities by either of the following methods: [102]

(a) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods:

[89] PCI DSS version 3.2 Requirement 6.5
[90] PCI DSS version 3.2 Requirement 6.5
[91] PCI DSS version 3.2 Requirement 6.5.1
[92] PCI DSS version 3.2 Requirement 6.5.2
[93] PCI DSS version 3.2 Requirement 6.5.3
[94] PCI DSS version 3.2 Requirement 6.5.4
[95] PCI DSS version 3.2 Requirement 6.5.5
[96] PCI DSS version 3.2 Requirement 6.5.6
[97] PCI DSS version 3.2 Requirement 6.5.7
[98] PCI DSS version 3.2 Requirement 6.5.8
[99] PCI DSS version 3.2 Requirement 6.5.9
[100] PCI DSS version 3.2 Requirement 6.5.10
[101] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[102] PCI DSS version 3.2 Requirement 6.6

a. At least annually; and
b. After any changes to the public facing website

(b) Installing an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic.

Supplemental Guidance: Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices.

- Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities
- Web-application firewalls filter and block nonessential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured.

An institution that specializes in "application security" can be either a third-party company or an internal team/department, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

UTEP does not currently host any public-facing web pages that are in scope.

PCI DSS CONTROL 6.7

Control Intent: The University ensures that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for developing and maintaining secure systems and applications are kept current and disseminated to all pertinent parties. [103]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

Please refer to the UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Account Management; Standard 7: Change Management; UTEP Standard 19: Server and Device Configuration and Management; UTEP Standard 21: System Development and Deployment; and The University of Texas at El Paso Minimum Security Standards for Systems.

[103] PCI DSS version 3.2 Requirement 6.7

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

To ensure critical 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" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS CONTROL 7.1

Control Intent: The University limits access to system components and cardholder data to only those individuals whose job requires such access.

Standard: Data custodians and data owners are required to implement administrative and technical measures to limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations include the following: [104]

(a) Defining access needs for each role, including: [105]
    1. System components and data resources that each role needs to access for their job function; and
    2. Level of privilege required (e.g., user, administrator, etc.) for accessing resources;
(b) Restricting access to privileged user IDs to least privileges necessary to perform job responsibilities; [106]
(c) Assigning access based on individual personnel's job classification and function; [107] and
(d) Requiring documented approval by authorized parties specifying required privileges. [108]

Supplemental Guidance: The implement of an automated access control system can be a combination of technology, since all modern computers, payment application, and Point of Sale (POS) software already have built-in systems for user accounts and privilege controls. Microsoft's PCI DSS Compliance Planning Guide should be referenced for using Active Directory as an automated access control system. [109]

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 10: Risk Management; Standard 11: Safeguarding Data; Standard 16: Data Center Security; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration and Management; Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, see Control 2.5 above for Vendor User Account Approval Form.

PCI DSS CONTROL 7.2

Control Intent: The University implements an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all," unless specifically allowed.

Standard: Data custodians and data owners are required to ensure systems components are configured to restrict 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: [110]

(a) Coverage of all system components; [111]
(b) Assignment of privileges to individuals based on job classification and function (RBAC); [112] and
(c) Default "deny-all" setting. [113]

Supplemental Guidance: Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges.

[104] PCI DSS version 3.2 Requirement 7.1
[105] PCI DSS version 3.2 Requirement 7.1.1
[106] PCI DSS version 3.2 Requirement 7.1.2
[107] PCI DSS version 3.2 Requirement 7.1.3
[108] PCI DSS version 3.2 Requirement 7.1.4
[109] Microsoft's Payment Card Industry Data Security Standard Compliance Planning Guide http://www.microsoft.com/en-us/download/details.aspx?id=18015
[110] PCI DSS version 3.2 Requirement 7.2
[111] PCI DSS version 3.2 Requirement 7.2.1
[112] PCI DSS version 3.2 Requirement 7.2.2
[113] PCI DSS version 3.2 Requirement 7.2.3

Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access.

Vendor manuals should be used to validate setting, since some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance

PCI DSS Control 7.3

Control Intent: The University ensures that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for restricting access to cardholder data are kept current and disseminated to all pertinent parties. [114]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally mandatory Institutional Compliance Training is performed on an annual basis. SAQs are also performed on an annual basis.

Requirement #8: Assign a Unique ID To Each Person With Computer Access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. These requirements are applicable for all accounts, including Point of Sale (POS) accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data.

PCI DSS Control 8.1

Control Intent: The University defines and implements policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.

Standard: Data custodians and data owners are required to assign all non-consumer users unique user identifications (ID) before allowing them to access system components. User identification controls include the following: [115]

(a) Controlling addition, deletion, and modification of user IDs, credentials, and other identifier objects; [116]
(b) Revoking access for any terminated users within twenty-four (24) hours of employment status change; [117]
(c) Removing or disabling inactive user accounts within ninety (90) days; [118]
(d) Managing user accounts assigned to vendors that are used to access, support, or maintain system components via remote access: [119]
    1. Enabling the accounts only during the time period needed and disabled when not in use; and
    2. Monitoring the accounts when in use;
(e) Limiting repeated access attempts be locked out after not more than six (6) invalid logon attempts; [120]
(f) Setting lockout durations to a minimum of thirty (30) minutes or until an administrator enables the user ID; [121] and
(g) Require users to re-authenticate if a session has been idle for more than fifteen (15) minutes to re-activate the terminal or session. [122]

[114] PCI DSS version 3.2 Requirement 7.3
[115] PCI DSS version 3.2 Requirement 8.1, 8.1.1
[116] PCI DSS version 3.2 Requirement 8.1.2
[117] PCI DSS version 3.2 Requirement 8.1.3
[118] PCI DSS version 3.2 Requirement 8.1.4
[119] PCI DSS version 3.2 Requirement 8.1.5
[120] PCI DSS version 3.2 Requirement 8.1.6
[121] PCI DSS version 3.2 Requirement 8.1.7
[122] PCI DSS version 3.2 Requirement 8.1.8

Supplemental Guidance: An example of uniqueness, the difference can be adding a designator to the end of the username, such as number. Examples include:

- First user in the system named "John Smith": John.Smith or JSMITH
- Second user in the system named "John Smith": John.Smith1 or JSMITH1
- Third user in the system named "John Smith": John.Smith2 or JSMITH2

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords (terminations); and Standard 22: Vendor and Third-Party Controls and Compliance

PCI DSS CONTROL 8.2

Control Intent: The University implements authentication mechanisms, in conjunction with unique IDs, to verify user legitimacy.

Standard: To ensure the proper management of user-authentication for non-consumer users and administrators on all system components, user authentication mechanisms shall:

(a) Use at least one of the following methods to authenticate all users in addition to assigning a unique ID: [123]
    1. Something you know, such as a password or passphrase;
    2. Something you have, such as a token device or smart card; or
    3. Something you are, such as a biometric;
(b) Use strong cryptography to render all authentication credentials unreadable during transmission and storage; [124]
(c) Verifying user identity before modifying any authentication credential that includes, but is not limited to: [125]
    1. Performing password resets;
    2. Provisioning new tokens; or
    3. Generating new keys;
(d) Requiring complex passwords/phrases are used that contains: [126]
    1. A minimum length of at least seven (7) characters; and
    2. Both numeric and alphabetic characters;
(e) Forcing password/phrase changes at least once every ninety (90) days; [127] and
(f) Prohibiting individuals from submitting a new password/phrase that is the same as any of the last four (4) passwords/phrases he or she has used; and [128]
(g) Setting passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. [129]

Supplemental Guidance: Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management. Passwords should never be written down or stored on-line in an unencrypted format.

Users must create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Strong (good) passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*)
- Eight (8) or more alphanumeric characters.
- Not a word in any language, slang, dialect, or jargon.
- Not based on personal information, names of family, or important calendar dates.

Weak (bad) passwords have the following characteristics:

- Default vendor password

[123] PCI DSS version 3.2 Requirement 8.2
[124] PCI DSS version 3.2 Requirement 8.2.1
[125] PCI DSS version 3.2 Requirement 8.2.2
[126] PCI DSS version 3.2 Requirement 8.2.3
[127] PCI DSS version 3.2 Requirement 8.2.4
[128] PCI DSS version 3.2 Requirement 8.2.5
[129] PCI DSS version 3.2 Requirement 8.2.6

- Contain less than seven (7) characters
- A word found in a dictionary (English or foreign)
- A common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
- The words "UTEP" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts or 123321)
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1 or 1secret)

Only individuals who have received prior approval from the Executive Vice President, Office of Legal Affairs, or Chief Information Security Officer (CISO) may perform password cracking on a periodic or random basis as part of the University's security testing procedures. If a password is guessed or cracked during one of these events, the user will be required to change it immediately.

Only portions of the control apply to UTEP. Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, Two-Factor Authentication (and then logon through the Shibboleth Federated Identity Solution) is mandatory for ALL remote access by personnel to on-campus resources. Annual Institutional Compliance training is also mandatory for all users.

PCI DSS CONTROL 8.3

Control Intent: The University requires two-factor authentication for remote access originating from outside the Cardholder Data Environment (CDE) the by employees, administrators, and third parties.

Standard: Data custodians are required secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication: [130]

(a) Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. [131]

(b) Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside UTEP's network. [132]

Supplemental Guidance: If remote access is to UTEP's network that has appropriate segmentation, such that remote users cannot access or impact the CDE, two-factor authentication for remote access to that non-CDE network would not be required. However, two-factor authentication is required for any remote access to networks with access to the CDE.

Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, Two-Factor Authentication (and then logon through the Shibboleth Federated Identity Solution) is mandatory for ALL remote access by personnel to on-campus resources. Annual Institutional Compliance training is also mandatory for all users.

PCI DSS CONTROL 8.4

Control Intent: The University documents and communicates authentication procedures and policies to all users.

Standard: In conjunction with the written policy and standards of the PCI DSS Information Security Policy, managers and supervisors are required to provide their staff with: [133]

(a) Guidance on selecting strong authentication credentials;
(b) Guidance for how users should protect their authentication credentials;
(c) Instructions not to reuse previously used passwords;

[130] PCI DSS version 3.2 Requirement 8.3
[131] PCI DSS version 3.2 Requirement 8.3.1
[132] PCI DSS version 3.2 Requirement 8.3.2
[133] PCI DSS version 3.2 Requirement 8.4

(d) Instructions to change passwords if there is any suspicion the password could be compromised.

Supplemental Guidance: Personnel need to be aware of and following security policies, standards, and operational procedures to ensure account credentials are properly protected to prevent unauthorized access to the network.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, Two-Factor Authentication (and then logon through the Shibboleth Federated Identity Solution) is mandatory for ALL remote access by personnel to on-campus resources. Annual Institutional Compliance training is also mandatory for all users.

PCI DSS CONTROL 8.5

Control Intent: The University does not use group, shared, or generic IDs, passwords, or other generic authentication methods.

Standard: UTEP's data custodians and data owners are prohibited from using group, shared, or generic IDs, passwords, or other authentication methods as follows: [134]

(a) Generic user IDs must be disabled or removed;
(b) Shared user IDs must not exist for system administration and other critical functions;
(c) Shared and generic user IDs must not be used to administer any system components; and
(d) Service providers with remote access to customer premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. [135]

Supplemental Guidance: If multiple users share the same authentication credentials (e.g., user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, Two-Factor Authentication (and then logon through the Shibboleth Federated Identity Solution) is mandatory for ALL remote access by personnel to on-campus resources. Annual Institutional Compliance training is also mandatory for all users.

PCI DSS CONTROL 8.6

Control Intent: The University ensures authentication mechanisms are used (e.g., passwords, pass phrases, physical or logical security tokens, smart cards, certificates, etc.) are assigned. [136]

Standard: Data custodians must have mechanisms in place to attribute access to an individual and when non-traditional user authentication mechanisms are used (e.g., physical or logical security tokens, smart cards, certificates, etc.), the use of these mechanisms must be controlled, as follows:

(a) Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
(b) Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

Supplemental Guidance: If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (e.g., a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 16: Data Center Security; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, Two-Factor Authentication (and then logon through the Shibboleth Federated Identity Solution) is mandatory for ALL remote access by personnel to on-campus resources. Annual Institutional Compliance training is also mandatory for all users.

[134] PCI DSS version 3.2 Requirement 8.5
[135] PCI DSS version 3.2 Requirement 8.5.1
[136] PCI DSS version 3.2 Requirement 8.6

Vulnerability scans are performed by the ISO on new systems prior to allowing them to go live; must pass scan for ISO to approve external DNS and port entries (performs basic account checking).

PCI DSS CONTROL 8.7

Control Intent: The University ensures that access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.

Standard: Data owners, in conjunction with data custodians, are required to restrict all access to any database containing cardholder data (including access by applications, administrators, and all other users), as follows: [137]

(a) All user access to, user queries of, and user actions on databases must be through programmatic methods;
(b) Only database administrators may have the ability to directly access or query databases; and
(c) Application IDs for database applications may only be used by the applications (not by individual users or other non-application processes).

Supplemental Guidance: Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who may need direct access to the database for their administrative duties).

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 16: Data Center Security; and Standard 19: Server and Device Configuration and Management. Additionally, annual Institutional Compliance training is also mandatory for all users.

PCI DSS CONTROL 8.8

Control Intent: The University ensures that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for identification and authentication are kept current and disseminated to all pertinent parties. [138]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 16: Data Center Security; and Standard 19: Server and Device Configuration and Management. Additionally, annual Institutional Compliance training is also mandatory for all users.

[137] PCI DSS version 3.2 Requirement 8.7
[138] PCI DSS version 3.2 Requirement 8.8

REQUIREMENT #9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, the following terminology applies:

- Onsite Personnel. This term refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises.
- Visitor. This term refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- Media. This term refers to all paper and electronic media containing cardholder data.
- Sensitive Area. This term refers to 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.

PCI DSS CONTROL 9.1

Control Intent: The University implements appropriate facility entry controls to limit and monitor physical access to systems in the Cardholder Data Environment (CDE).

Standard: Facility managers, in conjunction with data custodians, are required to implement appropriate facility entry controls to limit and monitor physical access to systems in the CDE, including but not limited to: [139]

(a) Using video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries: [140]
    1. Video surveillance footage must be readily accessible for at least three (3) months, unless otherwise restricted by law; and
    2. Access control mechanisms (e.g., sign-in sheets) must be readily accessible for at least three (3) months;

(b) Restricting physical access to publicly accessible network jacks, by either: [141]
    1. Preventing physical access to the network jack; or
    2. Disconnecting unused or publicly accessible network jacks at the patch panel;

(c) Restricting physical access to Wireless Access Points (WAPs), gateways, handheld devices, networking/communications hardware, and telecommunication lines. [142]

Supplemental Guidance: Access control mechanisms may be as simple as a sign-in sheet to monitor individual access to sensitive areas, if video surveillance capabilities are not available.

Please refer to UTEP Standard 4: Access Management (4.5-Data Access Control Requirements & 4.6); Standard 15: Passwords; Standard 16: Data Center Security; Standard 19: Server and Device Configuration and Management; Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 9.2

Control Intent: The University implements procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

Standard: UTEP's Human Resources (HR) department is responsible for develop procedures to easily distinguish between onsite personnel and visitors, including but is not limited to: [143]

(a) Identifying new onsite personnel or visitors (for example, assigning badges)
(b) Changes to access requirements
(c) Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

Supplemental Guidance: Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.

[139] PCI DSS version 3.2 Requirement 9.1
[140] PCI DSS version 3.2 Requirement 9.1.1
[141] PCI DSS version 3.2 Requirement 9.1.2
[142] PCI DSS version 3.2 Requirement 9.1.3
[143] PCI DSS version 3.2 Requirement 9.2

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 16: Data Center Security; and Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 9.3

Control Intent: The University implements physical access controls for onsite personnel to sensitive areas.

Standard: UTEP's Human Resources (HR) department is responsible for controlling physical access for onsite personnel to the sensitive areas as follows: [144]

(a) Access must be authorized and based on individual job function.
(b) Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

Supplemental Guidance: Controlling physical access to the CDE helps ensure that only authorized personnel with a legitimate business need are granted access. When personnel leave the institution, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to the CDE once their employment has ended.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 16: Data Center Security; and Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 9.4

Control Intent: The University implements procedures to identify, authorize and monitor visitors.

Standard: UTEP's Human Resources (HR) department is responsible for implementing procedures to identify, authorize and monitor visitors as follows: [145]

(a) Visitors must be authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained; [146]
(b) Visitors must be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel; [147]
(c) Visitors must be asked to surrender the badge or identification before leaving the facility or at the date of expiration; [148] and
(d) A visitor log must be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted:[149]
    1. The log must include:
        i. The visitor's name;
        ii. The firm represented; and
        iii. The onsite personnel authorizing physical access on the log; and
    2. This log must be maintained for a minimum of three (3) months, unless otherwise restricted by law.

Supplemental Guidance: Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities (and potentially, to cardholder data). Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 16: Data Center Security; and Standard 22: Vendor and Third-Party Controls and Compliance.

[144] PCI DSS version 3.2 Requirement 9.3
[145] PCI DSS version 3.2 Requirement 9.4
[146] PCI DSS version 3.2 Requirement 9.4.1
[147] PCI DSS version 3.2 Requirement 9.4.2
[148] PCI DSS version 3.2 Requirement 9.4.3
[149] PCI DSS version 3.2 Requirement 9.4.4

PCI DSS CONTROL 9.5

Control Intent: The University implements procedures to physically secure all media.

Standard: Data owners, in conjunction with data custodians, are required to physically secure all media, as follows: [150]

(a) Store media back-ups in a secure location, preferably an off-site facility, such as: [151]
    1. An alternate or back-up site; or
    2. A commercial storage facility; and
(b) Review the backup facility's security at least annually.

Supplemental Guidance: Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk. Media includes but is not limited to computers, removable electronic media, paper receipts, paper reports, and faxes.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 6: Backup and Disaster Recovery; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 19: Server and Device Configuration and Management; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, SAQs are reviewed annually at which time this information is reviewed with each merchant.

PCI DSS CONTROL 9.6

Control Intent: The University maintains strict control over the internal or external distribution of any kind of media.

Standard: Data owners, in conjunction with data custodians, are required to maintain strict control over the internal or external distribution of media, including the following: [152]

(a) Classifying media in accordance with Appendix A: Data Classification & Handling Guidelines so the sensitivity of the data can be determined; [153]
(b) Sending sensitive media by secured courier or other delivery method that can be accurately tracked; [154] and
(c) Ensuring prior management approval for any and all media that is moved from a secured area (including when media is distributed to individuals). [155]

Supplemental Guidance: Appendix A: Data Classification & Handling Guidelines covers the topics of data classification and handling in greater detail.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 6: Backup and Disaster Recovery; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 15: Passwords; Standard 19: Server and Device Configuration and Management; and Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 9.7

Control Intent: The University maintains strict control over the storage and accessibility of media.

Standard: Data owners, in conjunction with data custodians, are required to:

(a) Maintain strict control over the storage and accessibility of media; [156]
(b) Properly maintain inventory logs of all media; [157] and
(c) Conduct media inventories at least annually. [158]

Supplemental Guidance: Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.

[150] PCI DSS version 3.2 Requirement 9.5
[151] PCI DSS version 3.2 Requirement 9.5.1
[152] PCI DSS version 3.2 Requirement 9.6
[153] PCI DSS version 3.2 Requirement 9.6.1
[154] PCI DSS version 3.2 Requirement 9.6.2
[155] PCI DSS version 3.2 Requirement 9.6.3
[156] PCI DSS version 3.2 Requirement 9.7
[157] PCI DSS version 3.2 Requirement 9.7.1
[158] PCI DSS version 3.2 Requirement 9.7.1

Please refer to UTEP Standard 6: Backup and Disaster Recovery; Standard 7: Change Management; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 16: Data Center Security; and Standard 21: System Development and Deployment.

PCI DSS CONTROL 9.8

Control Intent: The University destroys media when it is no longer needed for business or legal reasons.

Standard: Data owners, in conjunction with data custodians, are required to sanitize media when it is no longer needed for business or legal reasons. Data custodians are required to destroy media that cannot be sanitized, as follows: [159]

(a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed; [160] or
    1. Secure storage containers must be used for cardholder data that is waiting to be destroyed.
(b) Render data on electronic media unrecoverable so that data cannot be reconstructed. [161]

Supplemental Guidance: Data destruction may be performed in-house or it may be outsourced to a qualified data destruction vendor. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 11: Safeguarding Data; Standard 17: Security Monitoring; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, please refer to the Electronic Data Destruction Guidelines, and UTEP Purchasing & General Services Records Management website: http://admin.utep.edu/Default.aspx?tabid=1677.

PCI DSS CONTROL 9.9

Control Intent: The University protects devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

Standard: Facility managers, in conjunction with data custodians and data owners, are required implement physical security controls and awareness training to protect devices that capture payment card data (e.g., Point of Sale (PoS) devices) via direct physical interaction with the card from tampering and substitution that includes, but is not limited to: [162]

(a) Maintaining an up-to-date list of devices that includes the following: [163]
    1. Make, model of device;
    2. Location of device (e.g., the address of the site or facility where the device is located); and
    3. Device serial number or other method of unique identification;
(b) Periodically inspecting device surfaces to detect tampering (e.g., addition of card skimmers to devices), or substitution (e.g., by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device); [164] and
(c) Providing training for personnel to be aware of attempted tampering or replacement of devices that includes the following: [165]
    1. Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices;
    2. Prohibiting the installation, replacement, or return devices without verification;
    3. Awareness for suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices); and
    4. Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g., to a manager or security officer).

Supplemental Guidance: Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will also try to add "skimming" components to the outside of devices, which are designed to capture payment card details before they even enter the device. For example, by attaching an additional card reader on top of the legitimate card reader so that the payment

[159] PCI DSS version 3.2 Requirement 9.8
[160] PCI DSS version 3.2 Requirement 9.8.1
[161] PCI DSS version 3.2 Requirement 9.8.2
[162] PCI DSS version 3.2 Requirement 9.9
[163] PCI DSS version 3.2 Requirement 9.9.1
[164] PCI DSS version 3.2 Requirement 9.9.2
[165] PCI DSS version 3.2 Requirement 9.9.3

card details are captured twice: once by the criminal's component and then by the device's legitimate component. In this way, transactions may still be completed without interruption while the criminal is "skimming" the payment card information during the process. Additional best practices on skimming prevention are available on the PCI SSC website.

Please refer to UTEP Standard 3: Information Security Program; Standard 9: Data Classification; Standard 10: Risk Management; Standard 11: Safeguarding Data; Standard 19: Server and Device Configuration and Management; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, any time a point of sale device changes custody it MUST be documented and an Equipment Custody Form (see below) must be filled out in its entirety. Only authorized individuals are allowed to pick up or access POS devices on campus and such access must be documented from the time the POS is received to when it is delivered and to whom. This information is reviewed on an annual basis when SAQs are renewed.

Equipment Custody Form – Information Security Office	
Equipment Received From	
1. (Name of Department):	2. (Location) :
3. (Contact Name) :	4. (Extension) :
5. (E-mail Address):	6. (Date) :
7. (Purpose) :	8. (Comments) :

UTEP Tag #	Item Serial Number	Item Description

Releasing Person (*if applicable*)	Person Taking Initial Custody
9. Printed Name :	10. Printed Name:

11. Signature :	12. Signature :

PCI DSS CONTROL 9.10

Control Intent: The University ensures that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. [166]

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for restricting physical access to cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

Same as 9.9 above.

[166] PCI DSS version 3.2 Requirement 9.10

REQUIREMENT #10: TRACK & MONITOR ALL ACCESS TO NETWORK RESOURCES & 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.

PCI DSS CONTROL 10.1

Control Intent: The University implements audit trails for linking access to system components to individual users.

Standard: Data custodians and data owners are required to implement auditing of systems and applications that allows access to system components to be linked to individual users. [167]

Supplemental Guidance: It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

Please refer to UTEP Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 16: Data Center Security; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration and Management; Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance.

PCI DSS CONTROL 10.2

Control Intent: The University utilizes automated audit trails for system components to reconstruct events.

Standard: Data custodians and data owners are required to implement automated audit trails for all system components to reconstruct the following events: [168]

(a) All individual user accesses to cardholder data; [169]
(b) All actions taken by any individual with root or administrative privileges; [170]
(c) Access to all audit trails; [171]
(d) Invalid logical access attempts; [172]
(e) Use of and changes to identification and authentication mechanisms, including but not limited to: [173]
    1. creation of new accounts and elevation of privileges; and
    2. all changes, additions, or deletions to accounts with root or administrative privileges;
(f) Initialization, stopping, or pausing of the audit logs; [174] and
(g) Creation and deletion of system-level objects. [175]

Supplemental Guidance: Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an institution to identify and trace potentially malicious activities.

Please refer to UTEP Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 16: Data Center Security; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration and Management; Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance.

[167] PCI DSS version 3.2 Requirement 10.1
[168] PCI DSS version 3.2 Requirement 10.2
[169] PCI DSS version 3.2 Requirement 10.2.1
[170] PCI DSS version 3.2 Requirement 10.2.2
[171] PCI DSS version 3.2 Requirement 10.2.3
[172] PCI DSS version 3.2 Requirement 10.2.4
[173] PCI DSS version 3.2 Requirement 10.2.5
[174] PCI DSS version 3.2 Requirement 10.2.6
[175] PCI DSS version 3.2 Requirement 10.2.7

PCI DSS CONTROL 10.3

Control Intent: The University follows best practices for logging audit trail entries.

Standard: Data custodians and data owners are required to configure systems to record at least the following audit trail entries for all system components for each event: [176]

(a) User identification; [177]
(b) Type of event; [178]
(c) Date and time; [179]
(d) Success or failure indication; [180]
(e) Origination of event; [181] and
(f) Identity or name of affected data, system component, or resource. [182]

Supplemental Guidance: By recording these details for the auditable events at PCI DSS requirement 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

Please refer to UTEP Standard 4: Access Management; Standard 7: Change Management; Standard 16: Data Center Security; Standard 17: Security Monitoring; and Standard 19: Server and Device Configuration and Management.

PCI DSS CONTROL 10.4

Control Intent: The University utilizes time-synchronization technology to synchronize all critical system clocks.

Standard: Network Time Protocol (NTP) is UTEP's official method of synchronizing all system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time:[183]

(a) Data custodians are responsible for configuring UTEP's NTP servers so that they are receiving time from industry-accepted time sources; [184] and
(b) Data owners must ensure NTP on their systems is configured properly and validate the following:
    1. Systems are configured to synchronize time with UTEP's NTP servers;
    2. Information systems have the correct and consistent time; [185] and
    3. Time data is protected from unauthorized modification. [186]

Supplemental Guidance: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[187] Official NIST or USNO Internet Time Service (ITS) that can to be used for system time synchronization include, but are not limited to:

- time.nist.gov 192.43.244.18 [primary]; and
- time-nw.nist.gov 131.107.13.100 [alternate]

Please refer to UTEP Network Time Protocol (NTP) Configuration Procedures (contact ISO for a copy) and UTEP Standard 19: Server and Device Configuration and Management. Additionally please refer to the UTEP Minimum Security Standards for Systems.

[176] PCI DSS version 3.2 Requirement 10.3
[177] PCI DSS version 3.2 Requirement 10.3.1
[178] PCI DSS version 3.2 Requirement 10.3.2
[179] PCI DSS version 3.2 Requirement 10.3.3
[180] PCI DSS version 3.2 Requirement 10.3.4
[181] PCI DSS version 3.2 Requirement 10.3.5
[182] PCI DSS version 3.2 Requirement 10.3.6
[183] PCI DSS version 3.2 Requirement 10.4
[184] PCI DSS version 3.2 Requirement 10.4.3
[185] PCI DSS version 3.2 Requirement 10.4.1
[186] PCI DSS version 3.2 Requirement 10.4.2
[187] http://tycho.usno.navy.mil/ntp.html

PCI DSS CONTROL 10.5

Control Intent: The University secures audit trails so logs cannot be altered.

Standard: Data custodians and data owners are required to secure audit trails so the logs cannot be altered. Securing audit trails includes the following: [188]

(a) Limiting viewing of audit trails to those with a job-related need; [189]
(b) Protecting audit trail files from unauthorized modifications; [190]
(c) As close to real-time as possible, backup or transfer audit trail files to a centralized log server or media that is difficult to alter; [191]
(d) Writing logs for external-facing technologies onto a secure, centralized, internal log server or media device; [192] and
(e) Using File Integrity Monitoring (FIM) or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. [193]

Supplemental Guidance: FIM or change detection software should be configured not to alert when new data is being added to logs, otherwise normal log traffic will generate change alerts on the log files.

Please refer to the UTEP Standard 4: Access Management (4.5); Standard 5: Administrative/Special Access Accounts; Standard 6: Backup and Disaster Recovery; Standard 16: Data Center Security: Standard 17: Security Monitoring; and Standard 19: Server and Device Configuration and Management. Additionally please refer to UTEP Minimum Security Standards for Systems.

PCI DSS CONTROL 10.6

Control Intent: The University implements a process to review logs and security events for all system components to identify anomalies or suspicious activity.

Standard: Data custodians and data owners are required to develop and implement a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes: [194]

(a) Reviewing the following, at least daily: [195]
    1. All security events;
    2. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    3. Logs of all critical system components; and
    4. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls
        ii. Intrusion Detection Systems (IDS)
        iii. Intrusion Prevention Systems (IPS)
        iv. Authentication servers (e.g., Active Directory domain controllers); and
        v. E-commerce redirection servers;
(b) Reviewing logs of all other system components periodically based on UTEP's policies and risk management strategy, as determined by UTEP's annual risk assessment; [196] and
(c) Following up exceptions and anomalies identified during the review process. [197]

Supplemental Guidance: Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.

The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

[188] PCI DSS version 3.2 Requirement 10.5
[189] PCI DSS version 3.2 Requirement 10.5.1
[190] PCI DSS version 3.2 Requirement 10.5.2
[191] PCI DSS version 3.2 Requirement 10.5.3
[192] PCI DSS version 3.2 Requirement 10.5.4
[193] PCI DSS version 3.2 Requirement 10.5.5
[194] PCI DSS version 3.2 Requirement 10.6
[195] PCI DSS version 3.2 Requirement 10.6.1
[196] PCI DSS version 3.2 Requirement 10.6.2
[197] PCI DSS version 3.2 Requirement 10.6.3

Please refer to the UTEP Standard 1: Information Resources Security Requirements and Accountability (1.7; 1.9); 4: Access Management (4.4; 4.5); Standard 5: Administrative/Special Access Accounts; Standard 17: Security Monitoring; and Standard 19: Server and Device Configuration and Management; and Standard 23: Security Control Exceptions. Additionally please refer to Security Exception Reporting Process.

PCI DSS CONTROL 10.7

Control Intent: The University retains audit trail history.

Standard: Data custodians and data owners are required to retain audit trail history for at least one (1) year, with a minimum of three (3) months immediately available for analysis. [198]

Supplemental Guidance: Logs are considered "immediately available" for analysis if the logs can be:

- Accessed online;
- Readily recovered from archived media; or
- Restorable from back-up.

Please refer to the UTEP Standard 4: Access Management (4.5); Standard 5: Administrative/Special Access Accounts; Standard 6: Backup and Disaster Recovery; Standard 16: Data Center Security: Standard 17: Security Monitoring; and Standard 19: Server and Device Configuration and Management. Additionally please refer to UTEP Minimum Security Standards for Systems.

PCI DSS CONTROL 10.8

Control Intent: The University is able to detect failures of critical security control systems in a timely manner.

Standard: Data custodians and data owners are required to:

(a) Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [199]
    1. Firewalls; IDS/IPS;
    2. FIM;
    3. Anti-malware;
    4. Physical access controls;
    5. Logical access controls;
    6. Audit logging mechanisms; and
    7. Segmentation controls (if used); and

(b) Develop processes for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [200]
    1. Firewalls;
    2. IDS/IPS;
    3. FIM;
    4. Anti-malware;
    5. Physical access controls;
    6. Logical access controls;
    7. Audit logging mechanisms; and
    8. Segmentation controls (if used).

Supplemental Guidance: Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.

The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

Please refer to UTEP Standard 1: Acceptable Use of Information Resources(1.10; 1.11; 1.12); Standard 8: Malware Prevention; Standard 11: Safeguarding Data; Standard 12: Security Incident Management; Standard 16: Data Center Security; Standard 17:

[198] PCI DSS version 3.2 Requirement 10.7
[199] PCI DSS version 3.2 Requirement 10.8
[200] PCI DSS version 3.2 Requirement 10.8.1

Security Monitoring; Standard 19: Server and Device Configuration and Management; Standard 21: System Development and Deployment; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, please refer to the UTEP Minimum Security Standards for Systems.

PCI DSS CONTROL 10.9

Control Intent: The University ensures that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. [201]

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for monitoring all access to network resources and cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

Institutional Compliance Training is mandated of all Faculty, Staff and Employees (e.g., Student Employees, Consultants, Third-Party Vendors, etc.) on an annual basis. The Compliance modules cover a variety of Institution-wide policies, standards, guidelines, as well as Federal and State regulations – including The University of Texas at El Paso Information Resources Use and Security Policy, Standards and Guidelines

REQUIREMENT #11: REGULARLY TEST SECURITY SYSTEMS & PROCESSES

Vulnerabilities are being discovered continually by malicious individuals and are being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect the changing environment.

PCI DSS CONTROL 11.1

Control Intent: The University implements processes to test for the presence of Wireless Access Points (WAPs) and detect and identify all authorized and unauthorized wireless access points.

Standard: Data custodians are required to implement a process to test for the presence of Wireless Access Points (WAPs) that includes: [202]

(c) Detecting and identifying all authorized and unauthorized wireless access points at least once every ninety (90) days;
(d) Maintaining an inventory of authorized WAPs including a documented business justification; [203] and
(e) Implementing incident response procedures in the event unauthorized WAPs are detected. [204]

Supplemental Guidance: Detection methods must be sufficient to detect and identify both authorized and unauthorized devices. Methods that may be used in the rogue WAPs (802.11) detection process includes, but are not limited to:

- Wireless network scans,
- Physical/logical inspections of system components and infrastructure,
- Network Access Control (NAC); or
- Wireless Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; 4: Access Management (4.2-4.4); Standard 17: Security Monitoring; and Standard 19: Server and Device Configuration and Management. Additionally, please refer to the UTEP Minimum Security Standards for Systems.

PCI DSS CONTROL 11.2

Control Intent: The University implements a process for running internal and external network vulnerability scans at least quarterly and after any significant change in the network.

[201] PCI DSS version 3.2 Requirement 10.9
[202] PCI DSS version 3.2 Requirement 11.1
[203] PCI DSS version 3.2 Requirement 11.1.1
[204] PCI DSS version 3.2 Requirement 11.1.2

Standard: Data custodians and data owners are required to perform the following vulnerability scanning-related activities: [205]

(a) Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel;[206]
(b) Perform 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; [207] and
(c) Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. [208]

Supplemental Guidance: A "quarter" is defined as a ninety (90) day period and a "significant change" in the network includes, but is not limited to:

- New system component installations;
- Changes in network topology;
- Firewall rule modifications; and
- Major product upgrades.

Please refer to Control 1.1 – UTEP Procedures for Requesting Static IP, DNS entries, and Firewall Changes; UTEP Standard 7: Change Management; Standard 17: Security Monitoring; and Standard 21: System Development and Deployment. External vulnerability scanning is provided on a quarterly basis by an Approved Scanning Vendor (ASV).

PCI DSS CONTROL 11.3

Control Intent: The University implements a methodology for penetration testing.

Standard: Data custodians and data owners are required to implement a methodology for penetration testing that includes the following:

(a) Coverage of all PCI DSS version 3.0 requirements: [209]
    1. Process is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115);
    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 PCI DSS 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 twelve (12) months; and
    8. Specifies retention of penetration testing results and remediation activities results.
(b) External penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [210]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;
(c) Internal penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [211]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;
(d) Exploitable vulnerabilities found during penetration testing must be corrected and testing shall be repeated to verify the corrections; [212] and

[205] PCI DSS version 3.2 Requirement 11.2
[206] PCI DSS version 3.2 Requirement 11.2.1
[207] PCI DSS version 3.2 Requirement 11.2.2
[208] PCI DSS version 3.2 Requirement 11.2.3
[209] PCI DSS version 3.2 Requirement 11.3
[210] PCI DSS version 3.2 Requirement 11.3.1
[211] PCI DSS version 3.2 Requirement 11.3.2
[212] PCI DSS version 3.2 Requirement 11.3.3

(e) If segmentation is used to isolate the CDE from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. [213]

Supplemental Guidance: This update to PCI DSS requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.

Procedures: Please refer to the UTEP Standard 1: Information Resources Security Requirements and Accountability (1.7); Standard 2: Acceptable Use of Information Resources; Standard 17: Security Monitoring; and UTEP Purchasing & General Services Records Management website: http://admin.utep.edu/Default.aspx?tabid=1677. External vulnerability scanning is provided on a quarterly basis by an Approved Scanning Vendor (ASV).

PCI DSS CONTROL 11.4

Control Intent: The University utilizes intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.

Standard: Data custodians and data owners are required to utilize Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to: [214]

(a) Prevent intrusions into the CDE;
(b) Monitor all traffic at the perimeter of the CDE, as well as at critical points in the CDE;
(c) Alert personnel to suspected compromises within the CDE; and
(d) Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

Supplemental Guidance: Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.

Please refer to Control 1.1 – UTEP Procedures for Requesting Static IP, DNS entries, and Firewall Changes; UTEP Standard 4: Access Management; Standard 7: Change Management; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration Management; and Standard 21: System Development and Deployment. External vulnerability scanning is provided on a quarterly basis by an Approved Scanning Vendor (ASV).

PCI DSS CONTROL 11.5

Control Intent: The University deploys change-detection mechanisms to alert personnel to unauthorized modifications.

Standard: Data custodians and data owners are required to deploy a change-detection mechanism (e.g., File Integrity Monitoring (FIM) tools) to: [215]

(a) Alert personnel to unauthorized modification of:
    1. Critical system files;
    2. Configuration files; or
    3. Content files;
(b) Configure the change-detection mechanism software to perform file comparisons at least weekly; and
(c) Implement a process to respond to any alerts generated by the change-detection mechanisms. [216]

Supplemental Guidance: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).
Examples of files that should be monitored:

- System executables;
- Application executables;

[213] PCI DSS version 3.2 Requirement 11.3.4 & 11.3.4.1
[214] PCI DSS version 3.2 Requirement 11.4
[215] PCI DSS version 3.2 Requirement 11.5
[216] PCI DSS version 3.2 Requirement 11.5.1

- Configuration and parameter files; and
- Centrally stored, historical or archived, log and audit files.

Please refer to Control 1.1 – UTEP Procedures for Requesting Static IP, DNS entries, and Firewall Changes; UTEP Standard 4: Access Management; Standard 7: Change Management; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration Management; and Standard 21: System Development and Deployment. Additionally, OSSEC is employed to capture when certain files types are modified.

PCI DSS CONTROL 11.6

Control Intent: The University ensures that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

Standard: Data custodians and data owners are required to ensure that the PCI DSS Information Security Policy and appropriate standards and procedures for security monitoring and testing are kept current and disseminated to all pertinent parties. [217]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources, under "Confidentiality & Security of Data"; and Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 11: Safeguarding Data; and Standard 22: Vendor and Third-Party Controls and Compliance. Additionally, users are required to complete Mandatory Institutional Compliance Training on an annual basis titled "Information Security and Protecting the Confidentiality of SSNs – UTS165". SAQs are also performed on an annual basis.

[217] PCI DSS version 3.2 Requirement 11.6

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

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, the term "personnel" refers to 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 (CDE).

PCI DSS CONTROL 12.1

Control Intent: The University establishes, publishes, maintains and disseminates a security policy.

Standard: UTEP's PCI DSS Information Security Policy fulfills the requirement within PCI DSS for a security policy. UTEP's CISO is responsible for the annual review of the PCI DSS Information Security Policy, as well as updates, as necessary. [218]

Supplemental Guidance: A UTEP Information Security Policy and Standards creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

While, UTEP's PCI DSS Information Security Policy establishes the documentation requirement for PCI DSS, the ISO are required to:

- Review and update the PCI DSS Information Security Policy, as needed; and
- Disseminate, and/or publish the PCI DSS Information Security Policy for staff and subordinates to ensure all UTEP personnel who interact with the CDE understand their requirements.

PCI DSS CONTROL 12.2

Control Intent: The University implements a risk-assessment process.

Standard: Data custodians and data owners are required to implement a risk-assessment process that: [219]

(a) Is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Identifies critical assets, threats, and vulnerabilities; and
(c) Results in a formal risk assessment.

Supplemental Guidance: Examples of risk assessment methodologies include but are not limited to

- OCTAVE;
- ISO 27005; and
- NIST SP 800-30.

Please refer to UTEP Standard 1: Acceptable Use of Information Resources (1.7-CISO; 1.9-Information Resources Owners; 1.10-Owner of Mission Critical Information Resources; 1.12-Information Security Administrator); Standard 3: Information Security Program; Standard 7: Change Management; Standard 9: Data Classification; Standard 10: Risk Management; Standard 16: Data Center Security; and Standard 21: System Development and Deployment.

PCI DSS CONTROL 12.3

Control Intent: The University develops and implements usage policies for critical technologies.

Standard: Data custodians and data owners are required to develop and implement usage policies for critical technologies and defining the proper use of these technologies. Usage policies require the following: [220]

(a) Explicit approval by authorized parties; [221]
(b) Authentication for use of the technology; [222]

[218] PCI DSS version 3.2 Requirements 12.1, 12.1.1
[219] PCI DSS version 3.2 Requirement 12.2
[220] PCI DSS version 3.2 Requirement 12.3
[221] PCI DSS version 3.2 Requirement 12.3.1
[222] PCI DSS version 3.2 Requirement 12.3.2

(c) A list of all such devices and personnel with access; [223]
(d) A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices); [224]
(e) Acceptable uses of the technology; [225]
(f) Acceptable network locations for the technologies; [226]
(g) List of University-approved products; [227]
(h) Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity; [228]
(i) Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use; [229] and
(j) For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. [230]

Supplemental Guidance: Appendix G: Rules of Behavior / User Acceptable Use covers UTEP's rules of behavior. Examples of critical technologies include, but are not limited to:

- Remote-access technologies;
- Wireless technologies;
- Removable electronic media
- Laptops;
- Tablets;
- Smart phones;
- Personal data/digital assistants (PDAs),
- E-mail usage; and
- Internet usage.

Please refer to UTEP Standard 2: Acceptable Use of Information Resources; Standard 4: Access Management; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 13: Use and Control of Social Security Numbers; Standard 15: Passwords; Standard 19: Server and Device Configuration and Management; Standard 23: Security Control Exceptions; and Standard 24: Disciplinary Actions. Additionally, refer to ISO System Hardening Guidelines; Web Application Guides and Hosted IT Services Checklist; and ISO Windows 10 OS Standalone Configuration Security Settings Guide (please contact ISO for a copy of these documents).

PCI DSS CONTROL 12.4

Control Intent: The University defines information security responsibilities for all personnel. [231]

Standard: UTEP's Human Resources (HR) department is required to ensure that information security policies, standards and procedures clearly define information security responsibilities for all personnel.

Supplemental Guidance: Information Security roles and responsibilities are defined in Appendix D: Information Security Roles & Responsibilities.

Please refer to The University of Texas at El Paso Information Resources Use and Security Policy, Standards; Guidelines; and The University of Texas at El Paso Handbook of Operating Procedures.

PCI DSS CONTROL 12.5

Control Intent: The University assigns an individual or a team information security management responsibilities.

[223] PCI DSS version 3.2 Requirement 12.3.3
[224] PCI DSS version 3.2 Requirement 12.3.4
[225] PCI DSS version 3.2 Requirement 12.3.5
[226] PCI DSS version 3.2 Requirement 12.3.6
[227] PCI DSS version 3.2 Requirement 12.3.7
[228] PCI DSS version 3.2 Requirement 12.3.8
[229] PCI DSS version 3.2 Requirement 12.3.9
[230] PCI DSS version 3.2 Requirement 12.3.10
[231] PCI DSS version 3.2 Requirement 12.4 & 12.4.1

Standard: UTEP's assigned Chief Information Security Officer (CISO) is required to perform or delegate the following information security management responsibilities: [232]

(a) Establish, document, and distribute security policies and procedures; [233]
(b) Monitor and analyze security alerts and information; [234]
(c) Distribute and escalate security alerts to appropriate personnel; [235]
(d) Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; [236]
(e) Administer user accounts, including additions, deletions, and modifications; [237] and
(f) Monitor and control all access to data. [238]

Supplemental Guidance: Information Security roles and responsibilities are defined in Appendix D: Information Security Roles & Responsibilities.

Please refer to UTEP Standard 1: Information Resources Security Requirements and Accountability (1.7)

PCI DSS CONTROL 12.6

Control Intent: The University implements a formal security awareness program.

Standard: UTEP's assigned Chief Information Security Officer (CISO), in conjunction with UTEP's Human Resources (HR) department, is required to develop and implement a formal security awareness program to make all personnel aware of the importance of cardholder data security, which includes: [239]

(a) Educating personnel upon hire and at least annually; [240] and
(b) Requiring applicable personnel to acknowledge at least annually that they have read and understand the PCI DSS Information Security Policy and procedures. [241]

Supplemental Guidance: Awareness methods can vary depending on the role of the personnel and their level of access to the cardholder data. If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.

Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.

Please refer to UTEP Standard 1: Information Resources Security Requirements and Accountability (1.7). Additionally annual Institutional Compliance training is provided to all employees and vendors.

PCI DSS CONTROL 12.7

Control Intent: The University screens potential personnel prior to hire to minimize the risk of attacks from internal sources.

Standard: UTEP's Human Resources (HR) department is responsible for screening potential personnel prior to hire to minimize the risk of attacks from internal sources. [242]

Supplemental Guidance: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. Examples of background checks include, but are not limited to:

- Previous employment history;
- Criminal record;

[232] PCI DSS version 3.2 Requirement 12.5
[233] PCI DSS version 3.2 Requirement 12.5.1
[234] PCI DSS version 3.2 Requirement 12.5.2
[235] PCI DSS version 3.2 Requirement 12.5.2
[236] PCI DSS version 3.2 Requirement 12.5.3
[237] PCI DSS version 3.2 Requirement 12.5.4
[238] PCI DSS version 3.2 Requirement 12.5.5
[239] PCI DSS version 3.2 Requirement 12.6
[240] PCI DSS version 3.2 Requirement 12.6.1
[241] PCI DSS version 3.2 Requirement 12.6.2
[242] PCI DSS version 3.2 Requirement 12.7

- Credit history; and Reference checks.

All individuals hired by The University of Texas at El Paso undergo a Criminal Background Check, to include Student employees. Please see The University of Texas at El Paso Handbook of Operating Procedures (Section V Human Resources, Chapter 12 Criminal Background Checks).

PCI DSS CONTROL 12.8

Control Intent: The University maintains and implements policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data.

Standard: Contract owners, in conjunction with data custodians and data owners, are required to maintain and implement policies and procedures to manage service providers that includes, but is not limited to: [243]

(a) Maintaining a list of service providers; [244]
(b) Maintaining a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of UTEP, or to the extent that they could impact the security of UTEP's CDE; [245]
(c) Ensures there is an established process for engaging service providers, including proper due diligence prior to engagement; [246]
(d) Maintaining a program to monitor service providers' PCI DSS compliance status at least annually; [247] and
(e) Maintaining information about which PCI DSS requirements are managed by each service provider, and which are managed by UTEP. [248]

Supplemental Guidance: If the entity shares cardholder data with service providers (e.g., back-up tape storage facilities, web hosting companies, or security service providers), the process of due diligence should include:

- Direct observations;
- Reviews of policies and procedures; and
- Reviews of supporting documentation.

Please refer to UTEP Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 10: Risk Management; Standard 16: Data Center Security; Standard 19: Server and Device Configuration and Management; Standard 21: System Development and Deployment; Standard 22: Vendor and Third-Party Controls and Compliance; and Non-Disclosure Agreement must be executed.

PCI DSS CONTROL 12.9

Control Intent: The University ensures service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Standard: UTEP's service providers are required to acknowledge in writing that they are responsible for the security of UTEP's cardholder data that the service provider possesses or otherwise stores, processes, or transmits on behalf of UTEP, or to the extent that they could impact the security of UTEP's CDE. [249]

Supplemental Guidance: This requirement is a best practice until June 30, 2015, after which it becomes a requirement. The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.

Please refer to the Non-Disclosure Agreement/contract which must be executed by all Vendors/Service Providers and the UTEP Purchasing and General Services webpage at: http://admin.utep.edu/Default.aspx?tabid=74496 AND PGS Terms and Conditions: http://admin.utep.edu/Default.aspx?PageContentID=5783&tabid=17953.

[243] PCI DSS version 3.2 Requirement 12.8
[244] PCI DSS version 3.2 Requirement 12.8.1
[245] PCI DSS version 3.2 Requirement 12.8.2
[246] PCI DSS version 3.2 Requirement 12.8.3
[247] PCI DSS version 3.2 Requirement 12.8.4
[248] PCI DSS version 3.2 Requirement 12.8.5
[249] PCI DSS version 3.2 Requirements 12.9

PCI DSS CONTROL 12.10

Control Intent: The University ensures an incident response capability exists and is prepared to respond immediately to potential cybersecurity incidents.

Standard: UTEP's Incident Response (IR) team is required to:

(a) Implement an IR capability that is prepared to respond immediately to potential cybersecurity incidents. [250]

(b) Create an IR plan that is capable of being implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: [251]

1. Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum;
2. Specific incident response procedures;
3. Business recovery and continuity procedures;
4. Data backup processes;
5. Analysis of legal requirements for reporting compromises;
6. Coverage and responses of all critical system components; and
7. Reference or inclusion of incident response procedures from the payment brands.

(c) Test the IR plan at least annually; [252]

(d) Designate IR personnel to be available on a 24/7 basis to respond to alerts; [253]

(e) Provide appropriate training to staff with security breach response responsibilities; [254]

(f) Include alerts from security monitoring systems, including but not limited to: [255]

1. Intrusion Detection Systems (IDS);
2. Intrusion Prevention Systems (IPS);
3. Firewalls; and
4. File Integrity Monitoring (FIM) systems; and

(g) Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. [256]

Supplemental Guidance: NIST guidance for incident response best practices can be referenced at:

- Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf)
- Guide to Integrating Forensic Techniques into Incident Response (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf)

Please refer to the UTEP Standard 1: Acceptable Use of Information Resources; Standard 6: Backup and Disaster Recovery; Standard 8: Malware Prevention; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 12: Security Incident Management as well as the Security Incident Management Process flowchart; Standard 16: Data Center Security; Standard 17: Security Monitoring; Standard 18: Security Training; Standard 22: Vendor and Third-Party Controls and Compliance; Security Incident Response; IRP Unit Plan*; the Business Impact Analysis*; and Disaster Preparedness Plan* (*please contact ISO for a copy of these documents).

PCI DSS CONTROL 12.11

Control Intent: The University ensures security control functionality by performing ongoing reviews of policies, standards and procedures.

Standard: UTEP's management is required to:

(a) Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:

(b) Daily log reviews;

1. Firewall rule-set reviews;
2. Applying configuration standards to new systems;

[250] PCI DSS version 3.2 Requirement 12.10
[251] PCI DSS version 3.2 Requirement 12.10.1
[252] PCI DSS version 3.2 Requirement 12.10.2
[253] PCI DSS version 3.2 Requirement 12.10.3
[254] PCI DSS version 3.2 Requirement 12.10.4
[255] PCI DSS version 3.2 Requirement 12.10.5
[256] PCI DSS version 3.2 Requirement 12.10.6

3. Responding to security alerts; and
4. Change management processes;

(c) Maintain documentation of quarterly review process to include:

1. Documenting results of the reviews; and
2. Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

Supplemental Guidance: Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.

The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.

Please refer to UTEP Standard 4: Access Management; Standard 5: Administrative/Special Access Accounts; Standard 7: Change Management; Standard 8: Malware Prevention; Standard 9: Data Classification; Standard 11: Safeguarding Data; Standard 12: Security Incident Management; Standard 16: Data Center Security; Standard 17: Security Monitoring; Standard 19: Server and Device Configuration Management; Standard 22: Vendor and Third-Party Controls and Compliance; and UTEP Minimum Security Standards for Systems.

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or Institutional directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
CONFIDENTIAL	Definition	Confidential information is highly-valuable, highly-sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Confidential information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to UTEP. · Impact could include negatively affecting UTEP's competitive position, violating regulatory requirements, damaging the University's reputation, violating contractual requirements, and posing an identity theft risk.
CONTROLLED EXTERNAL USE	Definition	Controlled information is highly-valuable, sensitive university information and the level of protection is dictated internally by UTEP
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Controlled information were to become available to unauthorized parties external to UTEP. · Impact could include negatively affecting UTEP's competitive position, damaging the University's reputation, violating contractual requirements, and exposing the geographic location of individuals.
CONTROLLED INTERNAL USE	Definition	Internal Use information is information originated or owned by UTEP, or entrusted to it by others. Internal Use information may be shared only with authorized individuals who are employed by the University and have a business need, but may not be released to the general public or external parties, due to the negative impact it might have on the University's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties internal to UTEP. · Impact could include damaging the University's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely sharable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to UTEP. · Impact would not be damaging or a risk to business operations.

A-2: Labeling

Labeling is the practice of marking an information system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material, since marketing material is primarily developed for public release.
- **Displayed**. Confidential or Controlled information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

A-3: General Assumptions

- Any information created or received by UTEP employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as Controlled "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification to the combined asset. For example, if an application contains Controlled Internal Use and Confidential information, the entire application is Confidential.
- Confidential and Controlled External Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Confidential information from a secured database to an unprotected Microsoft Excel spreadsheet.

A-4: Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
  - Passport number
  - Permanent resident card
- Driver License (DL)
- Financial account number
  - Payment card number (credit or debit)
  - Bank account number
- Electronic Protected Health Information (ePHI)

A-5: DATA HANDLING GUIDELINES

		CONTROLLED		
HANDLING CONTROLS	**CONFIDENTIAL**	**EXTERNAL USE**	**INTERNAL USE**	**PUBLIC**
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-UTEP employees.	▪ NDA is recommended prior to access by non-UTEP employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with University interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*

Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Confidential data. ▪ Posting to Internet sites is prohibited, unless it is pre-approved to contain Confidential data.	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*
Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*
Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside UTEP without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside the University without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of University-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

APPENDIX B: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

DATA CLASS	SENSITIVE DATA ELEMENTS	PUBLIC	INTERNAL CONTROLLED	EXTERNAL CONTROLLED	CONFIDENTIAL
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., University website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	
	Investment-Related Activity			X	
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X	
	Debt Amount Information			X	
	SEC Disclosure Information			X	

APPENDIX C: DATA RETENTION PERIODS

Please refer to the UTEP Data Retention Schedule published in the following UTEP website:
http://admin.utep.edu/Default.aspx?tabid=57519

SAMPLE

APPENDIX D: INFORMATION SECURITY ROLES & RESPONSIBILITIES

D-1: INFORMATION SECURITY ROLES

Every user at UTEP, regardless of position or job classification, has an important role, when it comes to safeguarding the Confidentiality, Integrity and Availability (CIA) of the Information Resources maintained by UTEP. It is important that every individual fully understand their role, their associated responsibilities, and abide by the security standards, policies, and procedures set forth by the PCI DSS Information Security Policy.

Role	Description of Security Role
Chief Information Security Officer (CISO)	The CISO is accountable to the UTEP senior management (e.g., President, Executive Vice President, Vice President for Information Resources and Planning) for the development and implementation of the Information Security Program. The CISO will be the central point of contact for setting the day-to-day direction of the Information Security Program and its overall goals, objectives, responsibilities, and priorities
Data Owners	Business or department manager with budgetary authority over the system(s) with responsibility for the basic operation and maintenance of the system(s).
Data Custodians	Under the direction of the CISO, data custodians (e.g., system and network administrators, Technology Implementation Managers-TIMs) are responsible for the technical implementation and management of the PCI DSS Information Security Policy. Party responsible for certain aspects of system security, such as adding and deleting user accounts, as authorized by the data owner, as well as normal operations of the system in keeping with job requirements.
End Users	All employees (and contractors) are considered both custodians and users of Information Resources on their issued information systems and are required to uphold all applicable PCI DSS Information Security Policy policies, procedures, standards, and guidelines.

D-2: INFORMATION SECURITY RESPONSIBILITIES

Responsibilities shall be assigned based on "ownership" or stake-holding by the Chief Information Security Officer (CISO).

Role	Description of Security Responsibility
President	▪ Oversee and approves the University's Information Security Program; ▪ Appoint, in writing, a Chief Information Security Officer (CISO) to implement the Information Security Program; ▪ Ensure an appropriate level of protection for all University owned or maintained Information Resources; whether retained in-house or under the control of contractors; ▪ Ensure that funding and resources are programmed for staffing, training, and support of the Information Security Program and for implementation of system safeguards, as required; ▪ Ensure that persons working in an information security role are properly trained, and supported with the appropriate resources; and ▪ Provide a secure processing environment including redundancy, backup and fault-tolerance services.
Chief Information Security Officer (CISO)	▪ Oversee and approve the University's Information Security Program including the employees, contractors and vendors who safeguard the University's Information Resources and data, as well as the physical security precautions for employees and visitors; ▪ Ensure an appropriate level of protection for the University's Information Resources; whether retained in-house or under the control of outsourced contractors; ▪ Issue the PCI DSS Information Security Policy policies and guidance that establish a framework for an Information Security Management System (ISMS); ▪ Identify protection goals, objectives and metrics consistent with corporate strategic plan; ▪ Ensure appropriate procedures are in place for Security Testing & Evaluation (ST&E) for all Information Resources; and monitor, evaluate, and report to UTEP management on the status of information security within the University; ▪ Ensure that persons working in an information security role are properly trained, and supported with the appropriate resources; ▪ Assist in compliance reviews and other reporting requirements;

	▪ Provide feedback to University management on the status of the Information Security Program, and suggest improvements or areas of concern in the program or any other security-related activity; ▪ Promote best practices in information security management; ▪ Monitor and evaluate the status of the University's information security posture by performing annual compliance reviews of the PCI DSS Information Security Policy and system controls (including reviews of security plans, risk assessments, security testing processes, and others); ▪ Provide security-related guidance and technical assistance to all operating units; ▪ Develop the Computer Incident Response Program (CIRP) and act as the University's central point of contact for incident handling, in concert with the University's Computer Incident Response Team (CIRT). ▪ Maintain liaison with external organizations on security-related issues; ▪ Identify resource requirements, including funds, personnel, and contractors, needed to manage the Information Security Program; and ▪ Assign ownership of resources.
Data Owner	▪ Include security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management); ▪ Ensure the security of data and application software residing on system(s); ▪ Develop and maintain security plans and contingency plans for all general support systems and major applications under their responsibility, which document the business associations and dependencies of their system (e.g., examine linked information resources and flow of information); ▪ Perform risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Conduct self-assessments of system safeguards and program elements and ensure certification and accreditation of the system; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Ensure system users have proper information security training (relevant to the system); ▪ Ensure IT contracts pertaining to the system include provisions for necessary security; ▪ Ensure that access to sensitive data is limited to those with a "need to know" or "need to use"; and ▪ Ensure systems' personnel are properly designated, monitored, and trained; ▪ Implement the system-level controls and maintain system documentation; ▪ Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management); ▪ Assist in the determination of an appropriate level of system and physical security commensurate with the level of sensitivity; ▪ Assist in the development and maintenance of security plans and contingency plans (e.g., Business Recovery Plans) for all general support systems and major applications under their responsibility; ▪ Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system; ▪ Attend security awareness training and programs; ▪ Maintain a cooperative relationship with business partners or other interconnected systems; ▪ Maintain an inventory of hardware and software; and ▪ Handle and investigate incidents in cooperation with and under direction of the Chief Information Security Officer (CISO)

Data Custodians (System and Network Administrators, and Technology Implementation Managers-TIMs)	▪ Assist in the development and maintenance of security plans and contingency plans for all general support systems and major applications under their responsibility; ▪ Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system; ▪ Evaluate proposed technical security controls to assure proper integration with other system operations; ▪ Identify requirements for resources needed to effectively implement technical security controls; ▪ Ensure integrity in implementing and operating technical security controls; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Read and understand all applicable training and awareness materials; ▪ Read and understand all applicable use policies or other rules of behavior regarding use or abuse of UTEP Information Resources; ▪ Develop system administration and operational procedures and manuals; ▪ Evaluate and develop procedures that assure proper integration of service continuity with other system operations; ▪ Inventory those systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, application administration, etc.); ▪ Know the sensitivity of the data they handle and take appropriate measures to protect it; and ▪ Know and abide by all applicable University policies, standards and procedures.
End Users	NOTE: end user's responsibilities center upon being aware of the sensitivity and proper handling method of sensitive information. ▪ Know and abide by all applicable policies and procedures; ▪ Complete all required user training and awareness programs; ▪ Understand and abide by the Rules of Behavior (see Appendix G); ▪ Know which systems or parts of systems for which they are directly responsible (printer, desktop, browser, etc.); ▪ Know the sensitivity of the data handled by systems under your control and take appropriate measures to protect it; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Follow labeling, handling, sharing, storage and destruction requirements based on appropriate classification / sensitivity level; ▪ When in doubt about the classification of specific information, ask your supervisor; ▪ Comply with all regulatory, business or legal data retention policies before disposing of information.

APPENDIX E: INFORMATION SECURITY EXCEPTION REQUEST PROCEDURES

The following procedure defines the process for the review and approval of exceptions to the PCI DSS Information Security Policy's policies, standards, guidelines, and procedures:

1. A manager (or an appointed designee) seeking an exception must assess the risks that non-compliance creates for the University. If the manager believes the risk is reasonable, then the manager prepares a written request describing the risk analysis and request for an exception (Note: The only reason to justify an exception is when compliance with a policy adversely affects business objectives or when the cost to comply offsets the risk of non-compliance). The risk analysis shall include:
    a. Identification of the threats and vulnerabilities, how likely each is to occur and the potential costs of an occurrence.
    b. The cost to comply.
2. Submit the request for exception to the Chief Information Security Officer (CISO) for review. The CISO will gather any necessary background information and make a recommendation to approve or deny the request. The CISO may recommend that other areas such as managers, data custodians, and legal representatives review certain decisions.
3. The CISO will approve or deny the request for an exception.
4. The requestor will be notified of the decision to approve or deny.
5. All requests for exception will be retained by the CISO.
6. Exceptions are valid for a one-year period unless otherwise noted. If the exception is still required, a manager or an appointed designee may seek to renew the exception and provide any additional risks identified since the previous request. If the conditions have substantially changed, a new request for exception must be submitted to the CISO. Where little has changed, the review process may be shortened as recommended by the CISO. Please refer to 1. above.

For additional information please refer to the UTEP Security Exception Reporting Process; and UTEP Standard 23: Security Control Exceptions.

APPENDIX F: TYPES OF SECURITY CONTROLS

F-1: PREVENTATIVE CONTROLS

Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information. Examples include, but are not limited to:

- Policy - Unauthorized network connections are prohibited.
- Firewall - Blocks unauthorized network connections.
- Locked wiring closet - Prevents unauthorized equipment from being physically plugged into a network switch.

F-2: DETECTIVE CONTROLS

Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Examples include, but are not limited to:

- Log monitoring and review – monitoring for anomalous traffic can detect unauthorized activity.
- System audit – monitoring for unauthorized changes can detect a breakdown in the change control process.
- File integrity checkers – monitoring for file changes can detect integrity compromises.
- Motion detection systems – monitoring for physical activity can detect a break in of a facility.

F-3: CORRECTIVE CONTROLS

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. In many cases the corrective security control is triggered by a detective security control. Examples include, but are not limited to:

- Procedures to clean a virus from an infected system.
- A guard checking and locking a door left unlocked by a careless employee.
- Updating firewall rules to block an attacking IP address as the attack is occurring.

F-4: RECOVERY CONTROLS

Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. Examples include, but are not limited to:

- After a disk failure, data is restored from a backup tape.
- A server automatically fails over to another server when a heartbeat (connectivity) is lost.

F-5: DIRECTIVE CONTROLS

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive Institutional information. Examples include, but are not limited to:

- Policy, standards, procedures, or guidelines.
- HR handbook, or UTEP Handbook of Operating Procedures (hoop)

F-6: DETERRENT CONTROLS

Deterrent security controls are controls that discourage security violations. Examples include, but are not limited to:

- An "Unauthorized Access Prohibited" sign may deter a trespasser from entering an area.
- The presence of security cameras might deter an employee from stealing equipment.
- A policy that states access to servers is monitored could deter unauthorized access.

F-7: COMPENSATING CONTROLS

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. Examples include, but are not limited to:

- If a specific server cannot have antivirus software installed because it interferes with a critical application, a compensating control would be to increase monitoring of that server or isolate that server on its own network segment.
- If a system is not able to restrict who can log onto it, network segmentation would be a compensating control to protect the rest of the network from the lack of access control on the system.

APPENDIX G: RULES OF BEHAVIOR / INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY

These Rules of Behavior apply to the use of UTEP-provided Information Resources, regardless of the geographic location:

- Data and information system use must comply with UTEP policies and standards.
- Unauthorized access to data and/or Information Resources is prohibited.
- Users must prevent unauthorized disclosure or modification of confidential and controlled information, including Personally Identifiable Information (PII).

G-1: INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY ACKNOWLEDGMENT

All individuals granted access to or use of UTEP System Information Resources must be aware of and agree to abide by the following acceptable use requirements (excerpt from UTEP Standard 2, the entire standard may be reviewed here: UTEP Standard 2: Acceptable Use of Information Resources):

Definitions	• University: The University of Texas at El Paso (referred to as "UTEP" or "the University") • System: The University of Texas System. • University Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. • University Data: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records. • Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law. • User: Any individual granted access to University Information Resources.
General	• University Information Resources are provided for the purpose of conducting the business of University and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by this policy. • Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice. • Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device. • All Users must comply with applicable University and System Information Resources Use and Security policies at all times. • Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law. • Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited. • Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas at El Paso." • Users should report misuse of University Information Resources or violations of this policy to their supervisors.
Confidentiality & Security of Data	• Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's Records Retention Policy and Records Management Guidelines. • Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties.

	• Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device. • In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements. • The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and U. T. System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology [or other applicable office] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations. • Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services. • Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University. • All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources. • Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.
Email	• Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements. • Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. • The following email activities are prohibited when using a University provided email account: o Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose. o Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University. o Sending or forwarding any email that is suspected by the User to contain computer viruses. o Any Incidental Use prohibited by this policy. o Any use prohibited by applicable University or System policy.
Incidental Use of Information Resources	• Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy. • Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts. • A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located. • Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited. • Incidental Use for purposes of political lobbying or campaigning is prohibited. • Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space). • Files not related to System business may not be stored on network file servers.
Additional Requirements for Portable and Remote Computing	• All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised. • University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to

	Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources • University issued mobile computing devices must be encrypted. • Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted. • University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources as soon as feasible. • Unattended portable computers, smart phones and other computing devices must be physically secured. • All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.
Password Management	• University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. • Each User is responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment

I acknowledge that I have received and read the Information Resources Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Signature: _____ Date_____

Print Name:_____

G-2: Additional Rules For Security & Privileged Users

Security and system administration personnel with elevated privileges have significant access to processes and data in Information Resources. As such, Security, Network, Systems, and Database Administrators have added responsibilities to ensure the secure operation of any UTEP system.

Personnel with elevated privileges are to:

- Advise the data owner on matters concerning information security.
- Assist the data owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to any information system that affect contingency and disaster recovery plans are conveyed to the data custodian responsible for maintaining continuity of operations plans for that information system.
- Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need to know basis.
- Verify that users have received appropriate security training before allowing access to any information system.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the Information Security Office (ISO).

For additional information please refer to The University of Texas at El Paso Information Resources Use and Security Policy and applicable standards, procedures and guidelines as may be applicable (e.g., UTEP Standard 1: Information Resources Security Requirements and Accountability; Standard 5: Administrative/Special Access Accounts; Standard 7: Change Management; Standard 19: Server and Device Configuration and Management; UTEP Minimum Security Standards for Systems; Change Management Guidelines, etc.)

APPENDIX H: RISK MANAGEMENT FRAMEWORK (RMF)

UTEP maintains an information security risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

H-1: RISK MANAGEMENT OVERVIEW

There is sometimes conflict between information security and other general system/software engineering principles. Information security can sometimes be construed as interfering with ``ease of use'' where installing security countermeasures take more effort than a ``trivial'' installation that works, but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.

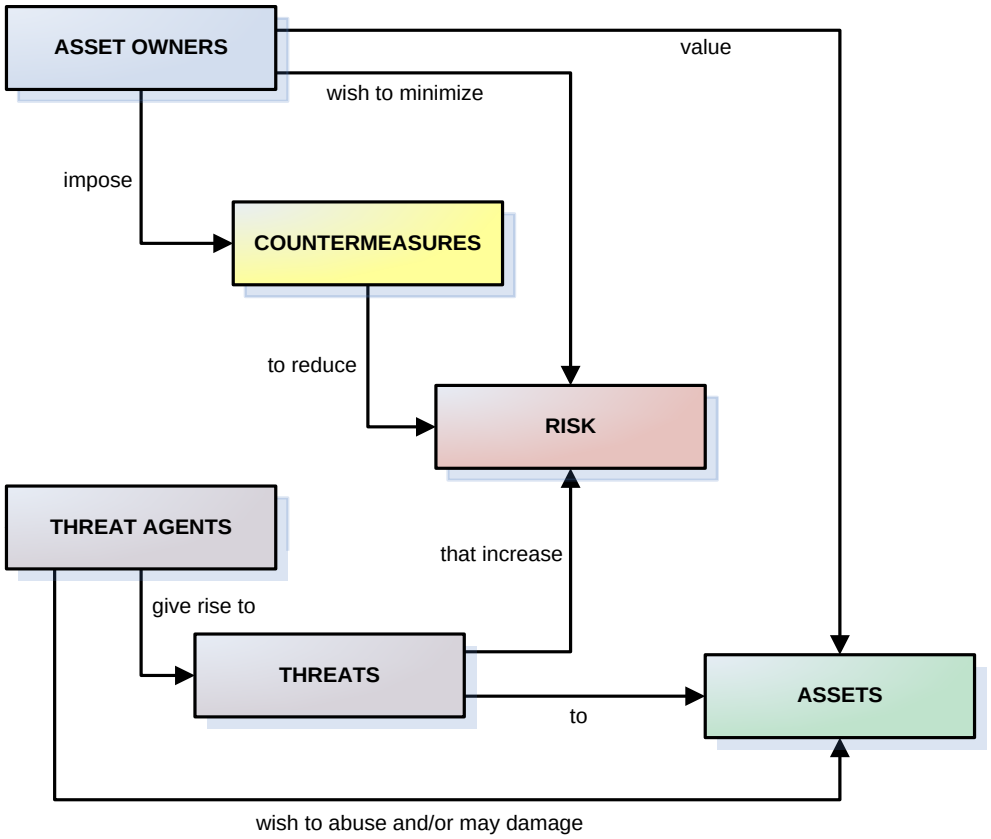


Figure H-1: Risk Overview

H-2: RISK MANAGEMENT FRAMEWORK (RMF)

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy information systems.

The Risk Management Framework (RMF) is based off of NIST SP 800-37[257]:

- **Categorize**. The information system and the information being processed, stored, and transmitted by the system, based on the potential impact to the University should events occur to put the system and its information at risk. The institution assigns a security impact value (low, medium, high) for the security objectives of confidentiality, integrity, or availability for the information resources that are needed by the University to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

- **Select**. An appropriate set of security controls are selected for the information system after categorizing and determining the minimum security requirements. Organizations meet the minimum security requirements by selecting an appropriately

[257] http://csrc.nist.gov/publications/PubsSPs.html

tailored set of baseline security controls based on an assessment of risk and local conditions, including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

- **Implement**. Security controls must be properly installed and configured in the information system. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment.

- **Assess**. Security Testing & Evaluation (ST&E) is used to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Authorize**. Based upon a determination of the risk to operations, organizational assets, or to individuals resulting from the operation of the information system and the determination that this risk is acceptable.

- **Monitor**. Assessing selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

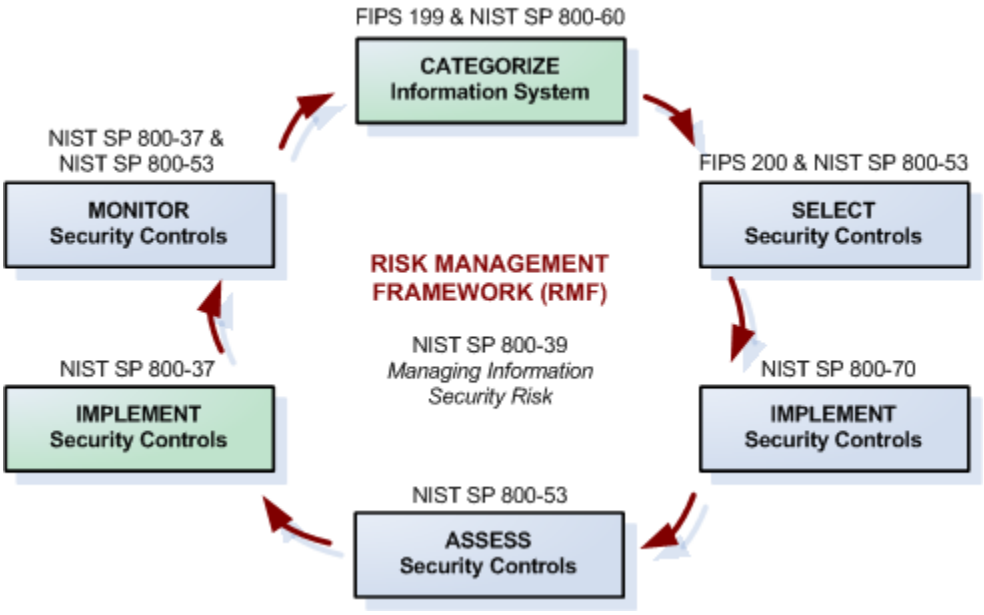


Figure H-2: Risk Management Framework (RMF)

H-3: Assessing Risk

UTEP must ensure that Risk Assessments (RAs) are conducted to identify the critical assets that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. RAs should take into account the potential adverse impact on UTEP's reputation, operations, and assets. RAs should be conducted by personnel associated with the activities subject to assessment.

RAs can be conducted on any system or project internal or external to UTEP, including applications, servers, networks, and any process or procedure by which these systems are administered and/or maintained. UTEP encourages authorized, periodic RAs for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

The execution, development and implementation of remediation programs are the responsibility of UTEP's management. Users are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.

A method of assessing risk is to identify the likelihood of an event actually taking place and the consequences that would result from the incident occurring.

While assessing the likelihood and consequence of an event is sometime more subjective, rather than based on quantifiable data, the following figures should be used to assess risk:

Rating Risk	EXTREME - detailed response plan & employee training required
	HIGH – requires management attention and response plan
	MODERATE – significant impact to overall operations
	LOW – managed by routine procedures
Likelihood	CERTAINTY - expected in most circumstances (matter of time)
	LIKELY – will probably occur in most circumstances
	POSSIBLE – could occur at some time
	UNLIKELY – not expected to occur
	RARE – exceptional circumstances only
Consequences	SEVERE – would stop achievement of functional goals & objectives
	MAJOR – would threaten functional goals & objectives
	MODERATE – significant impact to overall operations
	MINOR – would threaten an element of operations
	NEGLIGIBLE – minor impact on productivity

Figure H-3: Standardizing Terminology

Occurrence Probability		Occurrence Consequence				
		Negligible	**Minor**	**Moderate**	**Major**	**Severe**
	Certainty	**L**	**M**	**H**	**E**	**E**
	Likely	**L**	**M**	**H**	**E**	**E**
	Possible	**L**	**M**	**M**	**H**	**E**
	Unlikely	**L**	**M**	**M**	**M**	**H**
	Rare	**L**	**L**	**M**	**M**	**H**

Figure H-4: Risk Matrix

APPENDIX I: SYSTEM HARDENING

I-1: SERVER-CLASS SYSTEMS

Server-class systems are defined as:

- Microsoft Server 2000 – Deprecated; no longer authorized to be installed on UTEP systems
- Microsoft Server 2003 – Deprecated; no longer authorized to be installed on UTEP systems
- Microsoft Server 2008
- Microsoft Server 2012
- Redhat Enterprise Linux (RHEL)
- Debian (Linux)
- CentOS (Linux)
- Unix
- Solaris

Server-class systems should follow hardening procedures from the following sources:

- Center for Information Security (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Information Security Agency (DISA): http://iase.disa.mil/stigs/a-z.html
- Manufacturer security configuration recommendations

UTEP System Hardening, Web Application Guides and Hosted IT Services Checklist

I-2: WORKSTATION-CLASS SYSTEMS

Workstation-class systems are defined as:

- Microsoft XP – Deprecated; no longer permitted to be installed on University-owned/leased systems
- Microsoft Vista – Deprecated; no longer permitted to be installed on University-owned/leased systems
- Microsoft 7
- Microsoft 8
- Microsoft 10 only if ISO Windows 10 Standalone Configuration is applied (contact ISO)
- Windows 10 version 1507 – Deprecated; no longer permitted to be installed on University-owned/leased systems (as of March 26, 2017)
- Apple
- Fedora (Linux)
- Ubuntu (Linux)
- SuSe (Linux)
- Debian (Linux)
- CentOS (Linux)
- Mint (Linux)

Workstation-class systems should follow hardening procedures from the following sources:

- Center for Information Security (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Information Security Agency (DISA): http://iase.disa.mil/stigs/a-z.html
- Manufacturer security configuration recommendations
- UTEP Windows 10 Standalone Configuration

I-3: NETWORK DEVICES

Network devices are defined as:

- Firewalls
- Routers
- Load balancers
- Virtual Private Network (VPN) concentrators
- Wireless Access Points (WAPs)
- Wireless controllers
- Printers
- Multi-Function Devices (MFDs)

Network devices should follow hardening procedures from the following sources:

- Center for Information Security (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Information Security Agency (DISA): http://iase.disa.mil/stigs/a-z.html
- Manufacturer security configuration recommendations

I-4: Mobile Devices

Mobile devices are defined as:

- Tablets
- Mobile phones
- Other portable electronic devices

Network devices should follow hardening procedures from the following sources:

- Center for Information Security (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Information Security Agency (DISA): http://iase.disa.mil/stigs/a-z.html
- Manufacturer security configuration recommendations

I-5: Databases

Databases are defined as:

- MySQL
- Windows SQL Server
- Windows SQL Express
- Oracle
- DB2

Network devices should follow hardening procedures from the following sources:

- Center for Information Security (CIS): https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
- Defense Information Security Agency (DISA): http://iase.disa.mil/stigs/a-z.html
- Manufacturer security configuration recommendations

Refer to ISO System Hardening, Web Application Guides and Hosted IT Services Checklist document
ISO Windows 10 OS Standalone Configuration Security Settings Guide (please contact ISO for a copy of these documents)

APPENDIX J: PCI DSS SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

J-1: SAQ OVERVIEW

For the authoritative reference, please go to: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

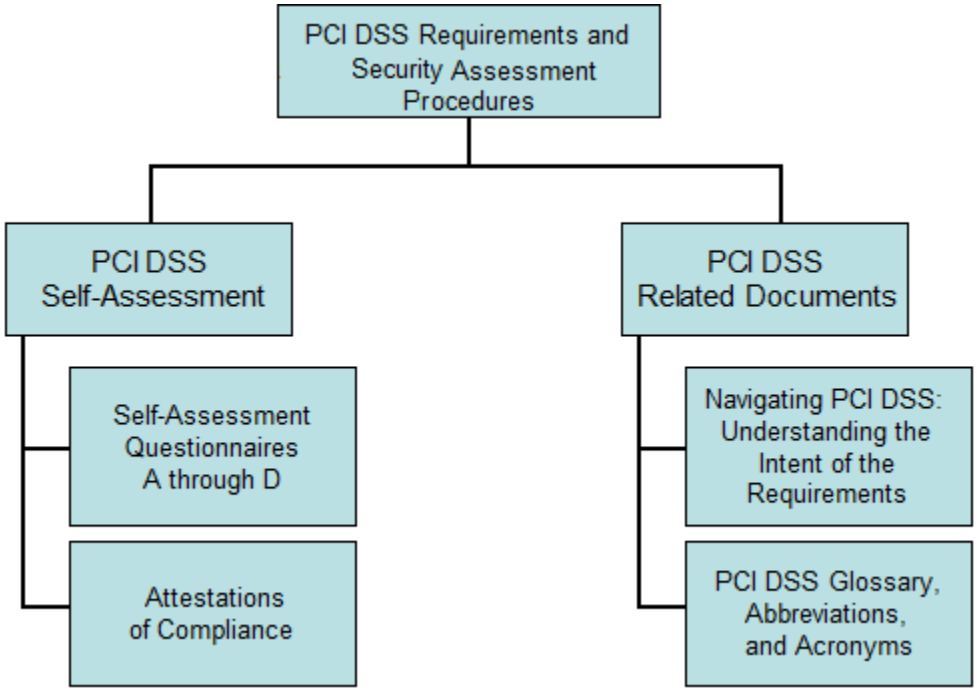
The PCI DSS SAQ is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS, and you may be required to share it with your acquiring bank. Please consult your acquirer for details regarding your particular PCI DSS validation requirements.

There are multiple versions of the PCI DSS SAQ to meet various business scenarios. A chart to help you determine which SAQ best applies to you and how to complete the SAQ is linked below, and is also included in the Instructions and Guidelines Document.

Each SAQ includes a series of yes-or-no questions about your security posture and practices. The SAQ allows for flexibility based on the complexity of a particular merchant's or service provider's business situation, as shown in the table below – this determines validation type. The SAQ validation type is not correlated with a merchant's classification or risk level.

Each Merchant must do the following three things, failure to comply may result in the merchant no longer approved to process credit card payments:

- Be compliant with the entire PCI DSS 3.2 requirements;
- Perform a Self-Assessment Questionnaire (SAQ), based on their Merchant type; and
- Sign an Attestation of Compliance (AoC)



J-2: HOW TO DETERMINE YOUR SAQ

For the authoritative reference, please go to: https://www.pcisecuritystandards.org/document_library?category=saqs#results

APPENDIX K: MANAGEMENT DIRECTIVE TEMPLATE

The University of Texas at El Paso
(UTEP**)**

PCI DSS Information Security Policy Implementation

The University of Texas at El Paso (UTEP) is committed to protecting its employees, partners, clients and UTEP from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every UTEP user who interacts with UTEP Information Resources. The reason for implementing UTEP's PCI DSS Information Security Policy is not to impose restrictions that are contrary to UTEP's established culture of openness, trust and integrity, but to strengthen UTEP's ability to guard against unauthorized access to, alteration, disclosure or destruction of Information Resources. This also includes against accidental loss or destruction.

The purpose of the PCI DSS Information Security Policy is to ensure that security controls are properly implemented and that clients and business partners are confident their information is adequately protected. Protecting University Information Resources, including the systems that collect, process, and maintain these resources are of critical importance. Therefore, the security of Information Resources must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – This security component addresses preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – This security component addresses the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – This security component addresses ensuring timely and reliable access to and use of information.

The PCI DSS Information Security Policy establishes the foundation for protecting cardholder data at UTEP. The formation of the policies is driven by many factors, with the key factor being risk. This policy sets the ground rules under which UTEP shall operate and safeguard its Information Resources to both reduce risk and minimize the effect of potential incidents.

This policy, including its related standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure UTEP users understand their day-to-day security responsibilities and the threats that could impact the Institution.

Implementing consistent security controls across the Institution will help UTEP comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity and availability of UTEP data.

It is the responsibility of every user to know this policy and to conduct their activities accordingly. The PCI DSS Information Security Policy is effective as of [enter date policy is effective].

Respectfully,

[owner/manager's signature]
[insert owner/manager's printed name]
[insert owner/manager's title]

APPENDIX L: USER ACKNOWLEDGEMENT FORM

The University of Texas at El Paso
(UTEP**)**

PCI DSS Information Security Policy Acknowledgement

I, _____, acknowledge I have read UTEP's PCI DSS Information Security Policy. I agree to abide by UTEP's policies, standard and procedures.

I acknowledge that if I do have any questions regarding any information within UTEP's PCI DSS Information Security Policy, it is my responsibility to address those issues with my manager for further clarification. I acknowledge that ignorance on my part is not an excuse and I take full responsibility for my actions and the actions I fail to do. I acknowledge and understand that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I agree to indemnify, defend and hold harmless UTEP, its subsidiaries and affiliated companies, and each of its respective owners, officers, directors, managers, employees, shareholders and agents (each an "indemnified party" and, collectively, "indemnified parties") from and against any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), and expenses (including, but not limited to, reasonable attorney's fees) threatened, asserted or filed by a third-party against any of the indemnified parties arising out of or relating to any and all gross negligence and/or misconduct on my part.

The terms of this acknowledgement shall survive any termination of employment.

User Name / Title	**Signature & Date**
User's Supervisor / Manager	**Signature & Date**

APPENDIX M: CERTIFICATION OF INFORMATION SECURITY AWARENESS TRAINING

Please refer to the Annual Institutional Compliance Training for Online Certification of awareness training maintained by the Institutional Compliance Office.

APPENDIX N: USER EQUIPMENT RECEIPT OF ISSUE TEMPLATE

The University of Texas at El Paso
(UTEP**)**

User Equipment Receipt of Issue

Item	Description	Qty	Make	Model	Serial #	Notes
1	Desktop					
2	Monitor					
3	Laptop w/ power cord					
4	Laptop case					
5	Docking station					
6	Cell phone w/ charger					
7	Printer					
8	Scanner					
9	Tablet					
10						
11						
12						
13						
14						
15						

Ownership:
I acknowledge that the item(s) listed in the table above, including all applicable software and licenses, remain the property of UTEP. These information assets are to be used solely in the execution of my official duties with UTEP. These information assets shall be accessible to UTEP upon demand and that UTEP may request and receive any and all of these items in my possession at any time.

Maintenance:
I acknowledge I am responsible to for the due care and due diligence in protecting these items from loss, theft, damage or compromise. I agree to keep UTEP informed of any repair or upgrade requirements.

If loss is deemed negligent on my behalf, I understand UTEP may seek financial reimbursement for the equipment based on the outcome of an investigation into the loss or damage of the information asset. I acknowledge that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I acknowledge my responsibilities for the equipment listed above and I verify the accuracy of the information associated with the items listed above (e.g. quantity, make, model, and serial #).

User Name / Title **Signature & Date**

User's Supervisor / Manager **Signature & Date**

NON-DISCLOSURE AGREEMENT

This non-disclosure agreement ("Agreement") is between **The University of Texas at El Paso** ("University"), a component of The University of Texas System ("System") and _____ ("Company"), a corporation having a business address at _____.

I. RECITALS

A. University has contracted with Company for the performance of certain services regarding _____ ("Services"), as a result of said performance of Services Company will have access to certain confidential education records as well as confidential, trade secrets, proprietary information and Covered Data and Information ("CDI") as defined below, (hereinafter collectively "Information") pertaining to the University, its faculty and students. This includes all communication of Information between the parties in any form whatsoever, including oral, written and machine readable form, pertaining to the above.

B. Covered Data and Information (CDI) includes paper and electronic student education record information supplied by University, as well as any data provided by University's students to the Company.

C. Company shall have access to the Information for the sole purpose of _____.

D. University is allowing access to the Information and Company is willing to receive the Information (as "Receiving Party") on the terms and conditions set forth herein.

II. AGREEMENTS

Therefore, University and Company agree, as follows:

1. Company acknowledges that it will be granted access to Information including yet not limited to CDI.

2. That the disclosure of Information by University is in strictest confidence and thus Company will:

a. Abide by the limitations on re-disclosure of personally identifiable information from education records set forth in The Family Educational Rights and Privacy Act (34 CFR §99.33 (a)(2)) and with the terms set forth below. 34 CFR §99.33 (a)(2) states that the officers employees and agents of a party that receives education record information from the University may use the information, but only for the purposes for which the disclosure was made;

b. Hold Information as well as CDI in strict confidence. Company shall not use or disclose Information received from or on behalf of University (or its students) except as permitted or required by law, or as otherwise authorized in writing by University. Company agrees not to use Information for any purpose other than the purpose for which the disclosure was made;

c. Not disclose to any other person the Information and use at least the same degree of care to maintain the Information secret as the Company uses in maintaining as secret its own secret information, but always at least a reasonable degree of care;

d. Use the Information only for the above purpose;

e. Restrict disclosure of the Information solely to those employees of Company having a need to know such Information in order to accomplish the purpose stated above;

f. Advise each such employee, before he or she receives access to the Information, of the obligations of Company under this Agreement as well as the University's Information Technology Acceptable Use Policy attached hereto as Exhibit "A" and as amended from time to time by the University, and require each such employee to maintain those obligations;

g. Develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Information including yet not limited to CDI received from, or on behalf of the University or its students;

h. Report to the University, within one business day of discovery, any use or disclosure of Information including yet not limited to CDI, not authorized by this Agreement or in writing by University. Company's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Information and/or CDI used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Company has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Company has taken or shall take to prevent future similar unauthorized use or disclosure. Company shall provide such other information, including a written report, as reasonably requested by University.

i. Upon request of University or termination, cancellation, expiration or any other conclusion of relationship between University and Company, return to University all Information including CDI, documentation, copies, notes, diagrams, computer memory media and other materials containing any portion of the Information, or, if return is not feasible, destroy any and all Information including yet not limited to CDI. If the Company destroys the Information, the Company shall provide University with a certificate confirming the date of destruction of the data and Information;

j. Immediately upon sale of Company or merger of Company with a third party, return to University all documentation, copies, notes, diagrams, computer memory media and other materials containing any portion of the Information, or confirm to University, in writing, the destruction of such materials;

3. This Agreement imposes no obligation on Company with respect to Information which (a)(1) was known to the Company prior to disclosure by University and (2) as to which the Company has no obligation not to disclose or use it, (b) is lawfully obtained by the Company from a third party under no obligation of confidentiality, (c) is or becomes generally known or available other than by unauthorized disclosure, (d) is independently developed by the Company or (e) is generally disclosed by University to third parties without any obligation on the third parties.

4. This Agreement imposes no obligation on Company with respect to any portion of the Information disclosed by University, unless such portion is (a) disclosed in a written document or machine readable media marked "CONFIDENTIAL" at the time of disclosure; (b) disclosed in any other manner and

summarized in a memorandum mailed to the Company within thirty (30) days of the disclosure or (c) is part of any information recorded or stored in any way in the University records, including handwriting, print, computer media, video or audio tape, film, microfilm and microfiche. Information disclosed by University in a written document or machine readable media and marked "CONFIDENTIAL" includes, but is not limited to, the items, if any, set forth in Schedule A attached hereto. Schedule A is incorporated herein by reference. Company hereby acknowledges receipt of the items listed in Schedule A, if any.

5. The Information shall remain the sole property of University.

6. UNIVERSITY DOES NOT MAKE ANY REPRESENTATION WITH RESPECT TO AND DOES NOT WARRANT ANY INFORMATION PROVIDED UNDER THIS AGREEMENT, BUT SHALL FURNISH SUCH IN GOOD FAITH. WITHOUT RESTRICTING THE GENERALITY OF THE FOREGOING, UNIVERSITY DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES, WHETHER WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED WITH RESPECT TO THE INFORMATION WHICH MAY BE PROVIDED HEREUNDER, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. UNIVERSITY SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY NATURE WHATSOEVER RESULTING FROM RECEIPT OR USE OF THE INFORMATION BY THE COMPANY.

7. If University reasonably determines in good faith that Company has materially breached any of its obligations under this contract, University, in its sole discretion, shall have the right to require Company to submit to a plan of monitoring and reporting; provide the Company with a fifteen (15) day period to cure the breach; or terminate any agreement immediately if cure is not possible. Before exercising any of these options, University shall provide written notice to Company describing the violation and the action it intends to take. If the Family Policy Compliance Office of the U.S. Department of Education determines that the Company improperly disclosed personally identifiable information obtained from Institution's education records, Institution may not allow the Company access to education records for at least five (5) years.

8. In the event of a breach or threatened breach or intended breach of this Agreement by Company, University, in addition to any other rights and remedies available to it at law or in equity, shall be entitled to preliminary and final injunctions, enjoining and restraining such breach or threatened breach or intended breach.

9. Company shall defend and hold University harmless from all claims, liabilities, damages, or judgments involving a third party, including University's costs and attorney fees, which arise as a result of Company's failure to meet any of its obligations under this Agreement.

10. The validity, construction, and performance of this Agreement are governed by the laws of the state of Texas.

11. The rights and obligations of the parties under this Agreement may not be sold, assigned or otherwise transferred.

12. If any arbitration, litigation or other legal proceeding relating to this Agreement occurs, the prevailing party shall be entitled to recover from the other party (in addition to any other relief awarded or granted) its reasonable costs and expenses, incurred in the proceeding.

13. This Agreement is binding upon University and Company, and upon the directors, officers, employees and agents of each. This Agreement is effective as of the later date of execution and will continue indefinitely,

unless terminated on thirty (30) days written notice by either party. However, Company's obligations of confidentiality and restrictions on use of the Information disclosed by University shall survive termination of this Agreement.

The University of Texas at El Paso

By:_____ Date:_____
Name:_____
Title:_____

(Company)

By:_____ Date:_____
Name:_____
Title:_____

EXHIBIT A

UTEP Standard 2: Acceptable Use of Information Resources

OGC REVISED FINAL June 18, 2014

The University of Texas at El Paso

INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by the following acceptable use requirements:

Definitions	• University: The University of Texas at El Paso (referred to as "UTEP" or "the University") • System: The University of Texas System. • University Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. • University Data: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records. • Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law. • User: Any individual granted access to University Information Resources.
General	• University Information Resources are provided for the purpose of conducting the business of University and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by this policy. • Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice. • Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device. • All Users must comply with applicable University and System Information Resources Use and Security policies at all times. • Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law. • Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited. • Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas at El Paso."

	• Users should report misuse of University Information Resources or violations of this policy to their supervisors.
Confidentiality & Security of Data	• Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's Records Retention Policy and Records Management Guidelines. • Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties. • Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device. • In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements. • The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and U. T. System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology [or other applicable office] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations. • Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services. • Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University. • All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources. • Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.
Email	• Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements. • Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. • The following email activities are prohibited when using a University provided email account:

	o Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose. o Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University. o Sending or forwarding any email that is suspected by the User to contain computer viruses. o Any Incidental Use prohibited by this policy. o Any use prohibited by applicable University or System policy.
Incidental Use of Information Resources	• Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy. • Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts. • A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located. • Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited. • Incidental Use for purposes of political lobbying or campaigning is prohibited. • Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space). • Files not related to System business may not be stored on network file servers.
Additional Requirements for Portable and Remote Computing	• All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised. • University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources • University issued mobile computing devices must be encrypted. • Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted. • University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources as soon as feasible. • Unattended portable computers, smart phones and other computing devices must be physically secured. • All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.

Password Management	• University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. • Each User is responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment

I acknowledge that I have received and read the Information Resources Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment and/or contract.

Signature: _____ Date_____

Print Name:_____

APPENDIX P: PCI INCIDENT RESPONSE FORM

Information Security Office

The University of Texas at El Paso
Incident Response Form

Case#	
Report Date/Time	

Confidentiality

Distribution of this document is limited to *UTEP Information Security Office*. Access should only be granted to those with a business related need-to-know. If you have any questions pertaining to the distribution of this document, please contact UTEP Chief Information Security Officer, Gerard D Cochrane (gdcochrane@utep.edu).

Incident Type	Location of Occurrence

System Information

Tag#/Serial Number	Operating System	Location	Technical Contact

Point of Contact

Name	Title	Telephone Number	Email Address

NARRATIVE

(Please provide as much detailed information as possible-Who, What, When, Where, Why, How)

DAMAGE ASSESSMENT

STEPS TAKEN TO RESTORE SERVICE/REMEDY PROBLEM

TIME REQUIRED TO RESTORE SERVICE/REMEDY PROBLEM

RESOURCES USED

CHANGES REQUESTED/NEED TO UPDATE INFORMATION SECURITY PROCEDURES

HISTORICAL TIMELINE

EVIDENCE LOG

☐ log file(s)	☐ screen shot(s)	☐ virus code	☐ email	☐ print-out(s)
☐ hard drive(s)	☐ HD image(s)	☐ hardware	☐ other:	
☐ any collected evidence			☐ Communications Log Attached	

Reported By:	**Date:**	**Time:**
Approved By:	**Date:**	**Time:**

APPENDIX Q: CHIEF INFORMATION SECURITY OFFICER (CISO) APPOINTMENT ORDERS TEMPLATE

The University of Texas at El Paso
(UTEP**)**

Duty Description: The Chief Information Security Officer (CISO) is accountable to UTEP's senior management (e.g., President, Executive Vice President, and Vice President for Information Resources and Planning) for the development and implementation of the Information Security Program. The CISO will be the central point of contact for setting the day-to-day direction of the Information Security Program and its overall goals, objectives, responsibilities, and priorities.

Responsibilities:

- Oversee and approve the University's Information Security Program including the employees, contractors and vendors who safeguard the University's Information Resources and data, as well as the physical security precautions for employees and visitors;
- Ensure an appropriate level of protection for the University's Information Resources; whether retained in-house or under the control of outsourced contractors;
- Issue the PCI DSS Information Security Policy that establishes a framework for an Information Security Management System (ISMS);
- Identify protection goals, objectives and metrics consistent with corporate strategic plan;
- Ensure appropriate procedures are in place for Security Testing & Evaluation (ST&E) for all Information Resources; and monitor, evaluate, and report to UTEP senior management on the status of Information Security within the Institution;
- Ensure that persons working in an Information Security role are properly trained, and supported with the appropriate resources;
- Assist in compliance reviews and other reporting requirements;
- Provide feedback to UTEP management on the status of the Information Security Program, and suggest improvements or areas of concern in the program or any other security-related activity;
- Promote best practices in Information Security management;
- Monitor and evaluate the status of the University's Information Security posture by performing annual compliance reviews of the PCI DSS Information Security Policy and system controls (including reviews of security plans, risk assessments, security testing processes, and others);
- Provide security-related guidance and technical assistance to all operating units;
- Develop the Computer Incident Response Program (CIRP) and act as the Institution's central point of contact for incident handling, in concert with the University's Computer Incident Response Team (CIRT).
- Maintain liaison with external organizations on security-related issues;
- Identify resource requirements, including funds, personnel, and contractors, needed to manage the Information Security Program; and
- Assign ownership of resources.

Qualifications:

- Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the senior management team and who is able to communicate security-related concepts to a broad range of technical and non-technical staff; and
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.

APPENDIX R: ADMINISTRATOR ACCOUNT REQUEST FORM

The University of Texas at El Paso
(UTEP)

Information Security Office PCI DSS

Vendor/User Account Approval Form

Applicant Section

I understand that the access being granted through my administrative office staff account is assigned to me at the request of the Department Head. It is to be used only in connection with my assigned duties as a vendor, consultant, or otherwise an employee of UTEP and may be revoked without notice upon the request of the administrator. I understand and accept the following terms and conditions:

- I agree not to reveal my password nor allow anyone to use the account assigned to me. I am responsible for any changes made under my credentials.
- I agree to abide by the Payment Card Industry Data Security Standard (PCI DSS), as well as The University of Texas at El Paso PCI DSS Policy, and the Acceptable Use Agreement.
- I agree to maintain the security of customer information, including payment cardholder information such as payment card number, payment cardholder name, expiration date, and payment cardholder verification number. I agree to refer *all outside requests* for cardholder information to the Information Security Office.
- I agree to maintain the confidentiality of any and all data that I retrieve in the course of my duties, including data that I use for reporting purposes or in other software products.
- I agree that it is my responsibility to prevent unauthorized access and disclosure of the data within my possession.
- Access to administrative data will be determined by the requirements of my vendor agreement, and therefore I am only authorized to retrieve this data on a "need to know" basis.
- I agree to comply with all UTEP policies including but not limited to Information Security policies, University of Texas System policies, computer access standards, confidentiality of data standards, data entry standards, and data integrity standards.

I am aware that any violation of these policies or standards may lead to the immediate suspension of my computer privileges. I understand that unauthorized release of sensitive or restricted information is a breach of data security and may be cause for disciplinary action, up to and including termination of agreement, and may be subject to or include civil and criminal prosecution.

Applicant Information:

Signature: _____ Date: _____

Name: _____ Email: _____

Job Title: _____ Company: _____

Phone: _____ Bldg/Room: _____

Address:

Job Function or Special Instructions:

_____

_____

Department Head: I authorize a user id or the changes listed for the above person. I understand that it is my responsibility to make appropriate changes when there is a change in the applicant's status.

Dept. Head Signature: _____ Date: _____

Dept. Head Name (Please Print): _____

Please Fax this form to (915) 747-6101 or E-Mail to security@utep.edu

Approval: _____ **Date:** _____

Chief Information Security Officer

APPENDIX S: FULL CHANGE MANAGEMENT REQUEST FORM

The University of Texas at El Paso
(UTEP**)**

PCI Full Change Management Request Form

CHANGE REQUEST TYPE:
☐ Software ☐ Hardware ☐ Interface

INSTRUCTIONS
Completed forms should be submitted to your primary supervisor. Your supervisor will forward this to the IT department.

End User Information

End User Name:		Service Desk# (if applicable) Phone:	
Department:		Email Address:	

Machine Location

Please list the room of the machine(s) which are affected by this change requests.

Machine Location:	

Software

Platform: ☐ **Windows** ☐ **Macintosh** ☐ **Linux**

Existing Software:	Application Name:		Version:	
Description of Issues:				
New Software:	Application Name:		Version:	

Important Note: A copy of the license and software for each new software request must be submitted with this change request for non-site licensed software

Hardware (Additional Peripherals)

Type of Machine: ☐ PC ☐ Macintosh ☐ Linux

Type of Peripheral: ☐ Printer ☐ Scanner ☐ Other – please specify:

Description of Issues:

New Hardware: Make/Model: Serial No:

Requestor Signoff

As the end user specified on this form, I certify that the information provided in this document is both true and accurate. I also certify in the case of software changes that my department is in possession of sufficient licenses for the application.

The end user also recognizes they may be called upon to provide further information to complete this request. UTEP will undertake all best efforts to ensure that changes are implemented within the appropriate timeframe. However, the end user recognizes that should the end user fail to provide assistance in a timely manner when asked there will be unavoidable delays to the deployment of the requested changes.

End User Signature **X** Date: / /

End User's Supervisor

Completed By: (print name) Signature: **X** Date Received: / /

Enterprise Computing Systems Support / Departmental Systems Administrator Use Only

Received By: (print name) Signature: **X** Date Received: / /

Change Control Board Use Only (EC / TI / CISO / VPIRP)

Type of change: ☐ Minor/Pre-approved ☐ Major

CCB Outcome: ☐ Not Approved ☐ Approved

Approved By: (print name) Signature: **X** Date Approved: / /

APPENDIX T: CHANGE CONTROL BOARD (CCB) MEETING FORM (IF APPLICABLE – FORMAT MAY BE DIFFERENT AS NEEDED)

CCB Meeting Minutes

[***Insert date of meeting: Month DD, YYYY***]

MINUTES

[*Items discussed*]

Next meeting is scheduled for [*month dd, yyyy*]

ACTION ITEMS

The Action Items discussed at the [Insert date of meeting] meeting are as follows. Shaded areas identify the Action Items that were closed at the previous meeting. New Action Items are placed above previous items.

Action Item ID	Date Assigned	Assigned To:	Description	Resolution

REVIEWED CRS

See attached CR report or fill-in the table below for each CR reviewed.

Item #	CR #	Impact Code	Category	Description	Disposition

ATTENDEES

Name

APPENDIX U: PORTS, PROTOCOLS & SERVICES DOCUMENTATION FORM

Example: fill out the approved networking ports required for the system to operate

Port	Protocol	Service	Description
22	TCP	Secure Shell (SSH)	Used for secure logins & file transfers (SFTP)
25	TCP	Simple Mail Transfer Protocol (SMTP)	Email server
80	TCP / UDP	Hypertext Transfer Protocol (HTTP)	IIS web server
443	TCP	Hypertext Transfer Protocol over SSL (HTTPS)	IIS web server, webmail
3389	TCP	Remote Desktop Protocol (RDP)	Remote administration

Service Desk# (if applicable):

Port	Protocol	Service	Description

APPENDIX V: PCI INCIDENT RESPONSE PLAN (IRP) TEMPLATE

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

PLAN OBJECTIVES

The objective of Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update University policies, standards, procedures, and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

IRP ACTIONS

Incident Responders (IR) will be their experience and best judgment to respond to potential incidents in a manner consistent with the severity level posed by the incident. If necessary, the IR will obtain external assistance to help with the triage and cleanup operations.

INCIDENT DISCOVERY

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability • Unexplained connection losses • Network intrusion detection alerts • Host intrusion detection alerts (until the host is overwhelmed) • Increased network bandwidth utilization • Large number of connections to a single host • Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) • Firewall and router log entries • Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability • Unexplained connection losses • Network intrusion detection alerts • Increased network bandwidth utilization • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) • Firewall and router log entries • Packets with unusual source addresses • Packets with nonexistent destination addresses
DoS against the operating system of a particular host	• User reports of system and application unavailability • Network and host intrusion detection alerts • Operating system log entries • Packets with unusual source addresses
DoS against an application on a particular host	• User reports of application unavailability • Network and host intrusion detection alerts • Application log entries • Packets with unusual source addresses

Malicious Software (malware) Examples	You might be infected with malware if you see…
A virus that spreads through email infects a host.	• Antivirus software alerts of infected files • Sudden increase in the number of emails being sent and received • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted, or inaccessible files • Unusual items on the screen, such as odd messages and graphics • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A worm that spreads through a vulnerable service infects a host.	• Antivirus software alerts of infected files • Port scans and failed connection attempts targeted at the vulnerable service (e.g., open Windows shares, HTTP) • Increased network usage • Programs start slowly, run slowly, or do not run at all • System instability and crashes
A Trojan horse is installed and running on a host.	• Antivirus software alerts of Trojan horse versions of files • Network intrusion detection alerts of Trojan horse client-server communications • Firewall and router log entries for Trojan horse client-server communications • Network connections between the host and unknown remote systems • Unusual and unexpected ports open • Unknown processes running • High amounts of network traffic generated by the host, particularly if directed at external host(s) • Programs start slowly, run slowly, or do not run at all • System instability and crashes
Malicious mobile code on a Web site is used to infect a host with a virus, worm, or Trojan horse.	• Indications listed above for the pertinent type of malicious code • Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host.	• Unexpected dialog boxes, requesting permission to do something • Unusual graphics, such as overlapping or overlaid message boxes • Sudden increase in the number of emails being sent and received • Network connections between the host and unknown remote systems
A user receives a virus hoax message.	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person • No links to outside sources • Tone and terminology attempt to invoke panic or a sense of urgency • Urges recipients to delete certain files and forward the message to others

Unauthorized Access Examples	You might be experiencing unauthorized access on your system or network if you see…
Root compromise of a host	• Existence of unauthorized security-related tools or exploits • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems) • System configuration changes, including— - Process/service modifications or additions - Unexpected open ports - System status changes (restarts, shutdowns) - Changes to log and audit policies and data - Network interface card set to promiscuous mode (packet sniffing) - New administrative-level user account or group • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs, or file systems) • User reports of system unavailability • Network and host intrusion detection alerts • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Highly unusual operating system and application log messages • Attacker contacts the institution to say that he or she has compromised a host
Unauthorized data modification (e.g. Web server defacement)	• Network and host intrusion detection alerts • Increased resource utilization • User reports of the data modification (e.g., defaced Web site) • Modifications to critical files (e.g., Web pages) • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots) • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems)
Unauthorized usage of standard user account	• Access attempts to critical files (e.g., password files) • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts) • Web proxy log entries showing the download of attacker tools
Physical intruder	• User reports of network or system unavailability • System status changes (restarts, shutdowns) • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed) • Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host)
Unauthorized data access (e.g., database of customer information, password files)	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP, and other protocols • Host-recorded access attempts to critical files

Inappropriate Usage Examples	You might have identified inappropriate usage if you see…
Unauthorized service usage (e.g., Web server, file sharing, music sharing)	• Network intrusion detection and network behavior analysis software alerts • Unusual traffic to and from the host • New process/software installed and running on a host - Password cracking tools - Unauthorized website running - File transfer software - Peer-to-Peer (P2P) sharing software running • New files or directories with unusual names (e.g., "warez" server style names) • Increased resource utilization (e.g., CPU, file storage, network activity) • User reports • Application log entries (e.g., Web proxies, FTP servers, email servers)
Access to inappropriate materials (e.g., downloading pornography, sending spam)	• Network intrusion detection alerts • Eyewitness reports or complaints to management, HR, or ethics o Pornographic or explicit content displayed • Application log entries (e.g., Web proxies, FTP servers, email servers) • Inappropriate files on workstations, servers, or removable media
Attack against internal party	• Network intrusion detection alerts • Inside party reports (e.g. management, HR, or ethics) - Harassing email or text messages sent to internal users - Pornographic or explicit content sent to internal users • Network, host, and application log entries
Attack against external party	• Network intrusion detection alerts • Outside party reports - Harassing email or text messages sent to external users - Pornographic or explicit content sent to external users - External attack traffic traced back to the University • Network, host, and application log entries

COMMON EFFECTS OF ATTACKS

There are at least four primary effects of attacks that affect Information Security:

- Denial of Service. Any action that causes all or part of the network's service to be stopped entirely, interrupted, or degraded sufficiently to impact operations. Examples of denial of service include network jamming, introducing fraudulent packets, and system crashes and/or poor system performance, in which people are unable to effectively use computing resources.
- Loss / Alteration of Data or Programs. An example of loss or alteration of data or programs would be an attacker who penetrates a system, then modifies an Operating System-level program/configuration file (e.g. audit) so that the intrusion will not be detected.
- Compromise of Data. One of the major dangers of a computer security incident is that information may be compromised. The release of classified information to people without the proper clearance or formal authorization jeopardizes our nation's security. Efficient incident handling minimizes this danger.
- Loss of Trust in Computing Systems. Users may lose trust in computing systems and become hesitant to use one that has a high frequency of incidents or even a high frequency of events that cause the user to distrust availability or integrity.

INCIDENT RESPONSE CATEGORIES

There are generally six (6) stages of incident response:

- Preparation. The most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident before it occurs can save valuable time and effort in the long run.
- Identification. Identify whether or not an incident has occurred. If one has occurred, the Incident Response Team can take the appropriate actions. Identification may come from Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), File Integrity Monitoring Systems (FIMS), or manual observance of an incident.
- Containment. Involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause the destruction and loss of data. As soon as an incident is recognized, the Incident Response Team must immediately begin working on containment.
- Eradication. Removing the cause of the incident can be a difficult process. It can involve virus removal, removing user permissions, and/or dismissing employees.
- Recovery. Restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that systems are back to its normal condition.
- Follow-up. Some incidents require considerable time and effort. It is common that once the incident appears to be contained and remedied; there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow- up can support any efforts to prosecute those who have broken the law. This includes changing any policies that may need to be narrowed down or be changed altogether.

Type	Source	Description
Computer Security Software Alerts		
Technical	Network-based, host-based, and wireless IDS	Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) products are designed to identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use a set of attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
Technical	Antivirus, antispyware, and antispam software	Antivirus and antispyware software are designed to detect various forms of malicious code and prevent them from infecting hosts. When antivirus or antispyware software detects malicious code, it typically generates alerts. Current antivirus and antispyware products are effective at detecting and eradicating or isolating malicious code if their signatures are kept up to date.
Technical	File integrity checking software	Incidents may cause changes to important files; file integrity checking software can detect such changes. It works by using a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Technical	3rd Party Monitoring service	Some institutions pay a third party to monitor their publicly accessible services, including but not limited to, Web, Domain Name System (DNS) and FTP servers. The third party automatically attempts to access each service every so many minutes. If the service cannot be accessed, the third party alerts the institution using the methods specified by the institution, such as phone calls, pages, and emails.
Logs		
Technical	Operating system, security, and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs. Logs can provide a wealth of information, such as which accounts were accessed and what actions were performed.
Technical	Network device logs	Logs from network devices such as firewalls and routers are not typically used as a primary source of precursors or indications. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity.

Publicly Available Information		
Human	Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in the detection and analysis of new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities. Several organizations, such as US-CERT, CERT®/CC, IAIP, and the Department of Energy's Computer Incident Advisory Capability (CIAC), periodically provide threat update information through briefings, Web postings, and mailing lists.
Human	Information on incidents at other organizations	Reports of incidents that have occurred at other organizations can provide a wealth of information. There are Web sites and mailing lists where incident response teams and security professionals can share information regarding reconnaissance and attacks that they have seen. In addition, some organizations acquire, consolidate, and analyze logs and intrusion detection alerts from many other organizations.
People		
Human	Internal Users	Users, system administrators, network administrators, security staff, and others from within the institution may report signs of incidents. It is important to validate all such reports. Not only do users generally lack the knowledge to determine if an incident is occurring, but also even the best-trained technical experts make mistakes. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
Human	Other Organizations	Although few reports of incidents will originate from people at other organizations, they should be taken seriously. A classic example is an attacker who identifies a serious vulnerability in a system and either informs the organization directly or publicly announces the issue. Another possibility is that the organization might be contacted by an external party claiming someone at the organization is attacking it. External users may also report other indications, such as a defaced Web page or an unavailable service. Other incident response teams also may report incidents.

INCIDENT CATEGORIES

An incident will be categorized as one of ten severity levels. These severity levels are based on the impact to the University and can be expressed in terms of financial impact, impact to operations, impact to sales, or impact to the University's image.

CAT	Severity	Situation	Category Description	Response Action	Recovery Actions
0	Training	Exercise (e.g. Network Defense Testing)	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Depends on the type of exercise.	There are no recovery procedures required for this event.
1	Criminal	Illegal Content	This category is used to respond to any suspected incidents involving either: - the possession or transmission of child pornography; or - possible terrorist-related activities.	Stop the investigation immediately. The incident handler must cease work and call the local office for the FBI and follow the FBI's response instructions.	There are no recovery procedures required for this event.
2	Serious	Successful Host Compromise (privileged-level access)	This is a root or administrator-level compromise of a system. A successful event of this nature means the intruder has total control over the host and access to any and all data stored on it or on systems that trust this host.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by ISO.	Do not start recovery procedures until directed to do so by ISO. Normal recovery procedures from an event of this category is rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify ISO to arrange for a verification scan to be conducted.
3	Serious	Malicious Software (servers)	Any software code intentionally created or introduced into a server-class system for the distinct purpose of causing hard or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident of change anything on the system unless directed to do so by ISO.	Do not start recovery procedures until directed to do so by ISO. Normal recovery procedures from an event of this category is rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify ISO to arrange for a verification scan to be conducted.

4	Serious	Malicious Software (workstations)	Any software code intentionally created or introduced into a workstation-class system for the distinct purpose of causing hard or loss to the computer system, its data, or other resources. Examples are spyware, adware, viruses, Trojans, worms, etc.	The system must be disconnected from the network. It should NOT be turned off. ISO or Technology Support personnel will respond and follow University-approved procedures to remediate the malware infection.	Normal recovery procedures from an event of this category is rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. ISO to arrange for a verification scan to be conducted.
5	Serious	Denial of Service (DoS) Attack	A successful event of this nature means the intruder has successfully denied access to either the entire network, portion of the network, or to critical systems or data.	Determine the cause, if at all possible. Contact ISO for assistance in determining the source of the attack and removing the threat. Take no further action unless directed to do so by ISO.	Review logs and configurations to determine if there is anything that can be done to prevent further occurrences of this type of event and/or the cause of the current event.
6	Serious	Unauthorized Scan (internal network)	Any automated probe attacks (e.g. Nessus, Nmap, etc.)	Contact ISO for assistance in determining if the scan is unauthorized.	Review system event logs and/or network logs to determine if any systems responded to the probe or scan and what information may have been obtained by the unauthorized scanner.
7	Significant	Successful Host Compromise (user-level access)	This is a user-level compromise. A successful event of this nature means the intruder has access to data, applications, and systems which the users is allowed to access.	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident of change anything on the system unless directed to do so by ISO.	Do not start recovery procedures until directed to do so by ISO. Normal recovery procedures from an event of this category is rebuilding the system from original media, installing all required patches, and scanning for vulnerabilities before reattaching to the network. Notify ISO to arrange for a verification scan to be conducted.
8	Significant	Attempted Access (unsuccessful)	An unsuccessful attempt to access or compromise an information system. An event of this nature means the intruder attempted a known exploit or attempted to log in to an information system but was not successful in compromising it or in logging in.	No response is necessary. Report the event to ISO and include as much data as possible about the intruder and the attempted compromise or intrusion. Take no further action unless directed to do so by ISO.	There are no recovery procedures required for this event.

9	Significant	Poor Security Practice	Examples of poor security practices are root login using telnet, ftp or http; bad passwords; not using secure protocols to transfer sensitive data; downloading unauthorized software; peer-to-peer (P2P) software, etc.	The response depends on the event. The response ranges from disconnection from the network to a system rebuild, to no action required. An incident report should be sent to the department to follow appropriate actions (e.g. verbal or written counseling).	The recovery depends on the type of event.
10	Significant	Unknown	If the threat is unclear, use this category until the threat or situation is investigated and a final determination has been made.	Reassign to the proper category when a final determination is made.	Recovery is determined after the final determination and event category is determined.

ESCALATION LEVEL CONSIDERATIONS

Incident Response management must consider several characteristics of the incident before escalating the response to a higher level. These considerations include:

- Legal requirements for breach notification?
- How wide spread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact to UTEP?
- Will this negatively affect UTEP's image?

INCIDENT RESPONSE PROCESS

The Incident Response Process is an escalation process where as the impact of the incident becomes more significant or wide spread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.

Step		Responsible Entity	Incident Response Plan (IRP) Actions	Completed
Detection and Analysis Phase				
1	1.0	Anyone	Determine If an Incident Occurred	
	1.1	Anyone	Analyze the precursors and indications. (Appendix 16-1)	
	1.2	Anyone	Look for correlating information. (Appendix 16-2)	
	1.3	Anyone	Perform research (e.g. search engines, vendor knowledge base, peer review, etc.)	
	1.4	Anyone	As soon as the incident handler believes an incident has occurred, he/she must begin documenting the incident and gathering evidence.	
2	2.0	Anyone	Notify IT Support	
	2.1	Anyone	The incident handler contacts IT Support and provides available documentation and evidence.	
	2.2	IT Support	IT Support classifies the incident according to Appendix 16-1	
	2.3	IT Support	If the IT Support categorizes the event as a full investigation, the IT Support technician should create a case file.	
	2.4	IT Support	IT Support on-call analyst consolidates documentation and evidence and, if applicable, stores the documentation in the case folder for the incident.	
3	3.0	IT Support	Incident Prioritization	
	3.1	IT Support	IT Support prioritizes handling the incident based on the business impact.	
	3.2	IT Support	IT Support will identify which Information Resources have been affected and forecast which resources will be affected.	
	3.3	IT Support	IT Support will estimate the current and potential technical effect of the incident.	
4	4.0	IT Support	Incident Notification	
	4.1	IT Support	IT Support will contact affected data owners and business units, alerting them to the situation.	
5	5.0	Multiple Entities	Incident Escalation (If Required)	
	5.1	IT Support	If the incident is believed to be significant, the IT Support technician or data owner is responsible to notify management for escalation.	
	5.2	Management	Management is responsible for coordinating further incident escalation steps, as required.	
Containment, Eradication, and Recovery Phase				
6	6.0	IT Support	Secure, Document, Acquire, Preserve & Analyze Evidence (If Required)	
	6.1	IT Support	IT Support will follow its Standard Operating Procedures (SOP) for evidence seizure and analysis.	
7	7.0	Multiple Entities	Contain the Incident	

	7.1	IT Support	IT Support will work with affected data custodians and business units to determine a containment strategy.	
	7.2	Multiple Entities	Incident handlers will implement steps to contain the incident.	
8	8.0	Multiple Entities	Eradicate the Incident	
	8.1	Multiple Entities	Identify and mitigate all vulnerabilities that were exploited.	
	8.2	Multiple Entities	Remove malicious code, inappropriate materials, and other components.	
9	9.0	Multiple Entities	Recover From the Incident	
	9.1	Multiple Entities	Return affected systems to an operationally ready state.	
	9.2	Multiple Entities	Confirm that the affected systems are functioning normally.	
	9.3	Multiple Entities	If necessary, implement additional monitoring to look for future related activity.	
Post-Incident Activity Phase				
10	10.0	IT Support	Follow-Up Report	
	10.1	IT Support	IT Support will create a follow-up report and distribute it appropriately.	
11	11.0	Multiple Entities	After Action Review (AAR)	
	11.1	Multiple Entities	Hold an After Action Review (AAR) / "lessons learned" meeting involving all key players.	
	11.2	Multiple Entities	Update any changes needed to the Incident Response Plan (IRP) or other policy/procedure/standard.	

INCIDENT RESPONSE TEAM

To adequately respond to an intrusion or incident, predetermined teams should be formed to react to predetermined incident characteristics. As the situation develops and the impact becomes more significant, the various teams may be called to contribute.

Incident Response Team Roles and Descriptions
Incident Response Coordinator. Individual responsible for conducting and coordinating the Incident Response Plan (IRP).
Technical Support Team Lead. Individual responsible for providing assistance to IT support, which could include support personnel, outside contractors, or individual users.
Management Team Lead. Management representative responsible for interfacing with other managers/executives in areas, such as Legal, Human Resources, or other specialties, as required.

INCIDENT RESPONSE TEAM RESPONSIBILITIES

Incident Response Coordinator

- Receive and track all reported potential threats.
- Escalate Incident Response if the threat manifests itself.
- Determine relevant membership of the Technical Support Team.
- Alert applicable support institutions of the potential threat and any defensive action required.
- Alert management of the potential threat.
- Start a chronological log of events.
- Receive status from IT Support and report to management on a regular basis.

Technical Support Team:

- Monitor all applicable sources for alerts or notification of a threat.
- Determine initial defensive actions required.
- Notify the Incident Response Coordinator.
- Determine best course of action for the containment of the incident and eradication of the threat.
- Report actions taken and status to the Incident Response Coordinator.
- Continue to monitor all know sources for alerts looking for further information or actions to take to eliminate the threat.
- Continue reporting status and actions taken to the Incident Response Coordinator for the chronological log of events.
- Monitor effectiveness of actions taken and modify them as necessary.

Management Team:

- Assume responsibility for directing activities, in regards to the incident.
- Actively participate in Incident Response operations, based on the effects to business operations.
- Determine whether escalation appropriate.
- Determine when the risk has been mitigated to an acceptable level.
- Contact local authorities, if deemed appropriate.
- Initial breach notification procedures, if applicable.
- Ensure that all needed information is being collected to support legal action or financial restitution.

INCIDENT NOTIFICATION REQUIREMENTS

UTEP shall perform a review as needed of notification requirements to determine who must be contacted and the timeline for notification following the identification of a data breach:

- Applicable state breach notification regulatory requirements
- Applicable Federal breach notification regulatory requirements
- Contractual obligations for breach notification

POST INCIDENT

Following an incident, the Incident Response Coordinator should work with the Technical Support Team to prepare a report for management to include:

- Estimate of damage and impact.
- Action taken during the incident (not technical detail).
- Follow on efforts needed to eliminate or mitigate the vulnerability.
- Policies or procedures that require updating.
- Efforts taken to minimize liabilities or negative exposure.
- Provide the chronological log and any system audit logs requested by the Management Team.
- Document lessons learned and modify the Incident Response Plan (IRP) accordingly.
- Recommend disciplinary action in the case that the incident was from an internal source.

APPENDIX W: BUSINESS IMPACT ANALYSIS (BIA)

NOTE: Please contact the Information Security Office to request a copy of this document. This document is restricted and is For Official Use Only

APPENDIX X: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (DRP) PCI

NOTE: Please contact the Information Security Office to request a copy of this document. This document is restricted and is For Official Use Only

DISASTER RECOVERY PLAN (DRP)

A Disaster Recovery Plan (DRP) specifies emergency response procedures, including specifying individual responsibility for responding in emergency situations, and specifying procedures to enable team members to communicate with each other and with management during and after emergency.

DRP CLASSIFICATION &SCOPING REQUIREMENTS

The DRP requirements for critical assets are summarized below:

Disaster Recovery Plan (DRP) Summary				
Criticality		High	Medium	Low
Data Sensitivity	Confidential	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan
	Controlled External Use	Moderate security required; must be in Disaster Recovery Plan	Moderate security required; may be in Disaster Recovery Plan	Moderate security required; need not be in Disaster Recovery Plan
	Controlled Internal Use	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal security required; need not be in Disaster Recovery Plan
	Public	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal security required; need not be in Disaster Recovery Plan

Backup copies of data and software that are sufficient for recovery from an emergency situation pertaining to critical assets must be stored at a secure, external site providing standard protection against hazards such as fire, flood, earthquake, theft, and decay. Requirements and procedures for such offsite backup shall be included in the DRP, including procedures and authorities for obtaining access to such sites in the event of an emergency.

Disaster recovery requirements should be specified when establishing maintenance agreements with vendors supplying components of critical resources. Ensure that vendors can provide replacement components within a reasonable period of time, when planning system upgrades or deployments.

DRP DATA BACKUP AVAILABILITY

Backup copies of data and software must be sufficient to satisfy DRP requirements, application or other critical information asset processing requirements, and any functional requirements of any critical information data custodian dependent upon such data. Backup copies for disaster recovery purposes must be stored at a secure, off-site location that provides industry-standard protection. These backup requirements extend to all Information Resources and data necessary to be reconstituted in the event of disaster.

BUSINESS CONTINUITY PLAN (BCP)

The Business Continuity Plan (BCP) outlines the steps required to operate in the event of an unanticipated interruption of normal operations. Please contact the Information Security Office to request a copy of this document; which is For Official Use Only.

IDENTIFIED DISASTERS & EMERGENCY SITUATIONS

UTEP has examined several potential environmental disasters and emergency situations. The focus is on the level of business disruption, which could arise from each type of disaster.

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

BCP. Business Continuity Plan
PDCA. Plan-Do-Check-Act
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
DRP. Disaster Recovery Plan
IRP. Incident Response Plan
ISMS. Information Security Management System
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard

DEFINITIONS

The PCI Security Standards Council publishes the "Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms" website for PCI DSS specific terminology. [258]

The National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the approved reference document used to define common information security terms. [259]

[258] PCI Data Security Standard Glossary, Abbreviations and Acronyms - https://www.pcisecuritystandards.org/security_standards/glossary.php
[259] NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

RECORD OF CHANGES

Issue	Date	Pages Affected	Description
Initial	4/22/2015	All	Initial version. Complete rewrite for PCI DSS version 3.1
Complete	10/31/2016	All	Complete revision to comply with new PCI DSS Version 3.2
Revised	6/26/2017	All	Incorporated UTEP Information Security Policy and Standards, Procedures and Guidelines. Updated all links.
Approved	6/26/2017		Approved by Chief Information Security Officer
Revised	8/25/2017	7, 20, 24 & 67; 77-109	Clarify policy applicability based on individual PCI DSS SAQs requirements; fix minor formatting issues; substitute APPENDIX for ANNEX for consistency.
Approved	8/25/2017		Approved by Chief Information Security Officer