Appendixes

Information Technology Standard for PCI systems

Syracuse University – Information Technology and Services

PCI – Network Security Standard (Appendix 1)

1.0 Scope

- All credit card data and its storage media.
- This includes any card holder data and card identifying information including names address of credit card holder.

Data which meets the guidelines above are considered to be *in scope* for the Payment Card Industry Data Security Standard (PCI DSS), and must confirm to the Credit Card Data Transaction and Storage Standard.

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS V 3.2 requirements for system components considered to be in scope as defined in Section 1.0 of this document.

3.0 PCI Network Security Standard

The standard below sets forth a set of requirements for the credit card data processing and storage in SU PCI Network. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaire D* and by the SU PCI Committee.

3.1 Install and maintain a firewall configuration to protect cardholder data

3.1.1 Firewall and router configuration standards must be in place that include the following:

3.1.1.1 A formal change control process for approving, verifying and testing all external network connections and changes to the firewall and router configurations.

3.1.1.2 Change control processes to include verification of PCI DSS requirements impacted by a change.

3.1.1.3 A current network diagram documenting all connections to cardholder data, including wireless networks

3.1.1.3.1 This diagram must be updated regularly

3.1.1.4 A current diagram showing all cardholder data flows across systems and networks

3.1.1.5 Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone

3.1.1.6 Description of groups, roles and responsibilities for management of network components

3.1.1.7 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure (i.e. FTP, Telnet, POP3)

3.1.1.8 Insecure services, protocols and ports that are necessary for business as well as their security features must be documented, and the security features implemented.

3.1.1.9 Requirement for firewall and router configuration standards and rule sets to be reviewed every six months.

3.1.2 Firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment must be built

3.1.2.1 Inbound and outbound traffic must be restricted to that which is absolutely necessary for PCI business function, and these restrictions must be documented - all other inbound/outbound traffic must be denied

3.1.2.2 Router configuration files must be secure and synchronized

3.1.2.3 Perimeter firewalls must be installed between any wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the CDE

3.1.3 Prohibit direct public access between the internet and any system component in the CDE

3.1.3.1 A DMZ must be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports

3.1.3.2 Inbound internet traffic must be limited to IP addresses within the DMZ

3.1.3.3 Direct connections between the internet and cardholder data environment must be restricted

3.1.3.4 Do not allow unauthorized outbound traffic from the CDE to the internet

3.1.3.5 Stateful inspection must be implemented

3.1.3.6 System components storing cardholder data must be placed in an internal network zone segregated from the DMZ and other untrusted networks

3.1.3.7 Disclosure of private IP addresses and routing information to the internet to unauthorized parties must be prevented using methods such as the following:

3.1.3.7.1 Network Address Translation (NAT)

3.1.3.7.2 Proxy servers, firewalls or content caches

3.1.3.7.3 Removal or filtering of route advertisements

3.1.3.7.4 Internal use of RFC1918 address space

3.1.4 Personal firewall software or equivalent must be installed and active on any mobile and/or employee owned computers with direct connectivity for the internet when outside the network, and which are also used to access the network

3.1.4.1 Specific configuration settings are defined for personal firewall software

3.1.4.2 Personal firewall software is actively running

3.1.4.3 Personal firewall software is not alterable by users of mobile and/or employee-owned devices

3.1.5 Security policies and operational procedures for managing firewalls must be documented, in use, and known to all affected parties

3.2 Do not use vendor-supplied defaults for system passwords and other security parameters

3.2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, SNMP community strings, etc.

3.2.2 Wireless environments connected to the cardholder data environment or transmitting cardholder data must have their default configurations changed

3.2.2.1 Encryption keys must be changed from default at installation as well as each time an employee with knowledge of the keys leaves the company or changes position

3.2.2.2 Default SNMP community strings must be changed

3.2.2.3 Default passwords/passphrases on access points must be changed

3.2.2.4 Firmware on wireless devices must support strong encryption for authentication and transmission over wireless networks

3.2.2.5 Any other security-related wireless vendor defaults must be changed

3.2.3 Configuration standards developed for all system components must be consistent with industry standard system hardening standards (e.g., SANS, NIST, ISO, CIS)

3.2.4 Only one primary function may be implemented per server such that functions requiring different security levels do not co-exist on a single server (e.g., web servers, database servers, DNS)

3.2.4.1.1 If virtual technologies are used, only one primary function may be implemented per virtual system component/device

3.2.5 Only necessary services, protocols, daemons, etc. may be enabled as required for the function of the system – all others must be disabled

3.2.6 Implement additional security features for any requires services, protocols, or daemons that are considered to be insecure.

3.2.7 Configure security system parameters to prevent misuse

3.2.8 All unnecessary functionality must be removed such as scripts, drivers, features, subsystems, file systems and unnecessary web servers

3.2.9 Non-console administrative access must be encrypted using strong cryptography with technologies such as SSH, VPN or TLS1.2 for web-based management and other non-console administrative access

3.2.10 System services and parameter files must be configured to prevent the use of Telnet and other insecure remote login commands

3.2.11 Administrator access to web-based management interfaces must be encrypted with strong cryptography

3.2.12 Maintain an inventory of system components that are in-scope for PCI DSS

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

3.2.14 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.

4.0 Referred Documents, Web Pages and Contact Information

Item	Location/Info
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214
Guideline: *PCI DSS Self-Assessment Questionnaire D v3.2*	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Syracuse University Information Technology Standard for PCI systems	http://its.syr.edu/security/standards/PCIstandard.pdf
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	October, 1, 2016

Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 31st, 2017

Information Technology Standard for PCI systems
Syracuse University – Information Technology and Services
PCI – Credit Card Handling Standard (Appendix 2)

1.0 Scope

- All credit card data and its storage media.
- This includes any card holder data and card identifying information including names address of credit card holder.

Data which meets the guidelines above are considered to be *in scope* for the Payment Card Industry Data Security Standard (PCI DSS), and must confirm to the Credit Card Data Transaction and Storage Standard.

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS V 3.2 requirements for system components considered to be in scope as defined in Section 1.0 of this document.

3.0 PCI Network Security Standard

The standard below sets forth a set of requirements for the credit card data processing and storage in SU PCI Network. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaire D* and by the SU PCI Committee.

3.1 Protect stored cardholder data

3.1.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data storage:

3.1.1.1 Limit data storage amount and retention time to that which is required for legal, regulatory and business requirements

3.1.1.2 Process must exist for secure deletion of data when no longer needed

3.1.1.3 Specific retention requirements for cardholder data

3.1.1.4 A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention

3.1.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process

3.1.3 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)

3.1.4 Do not store 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

3.1.5 Do not store the personal identification number (PIN) or the encrypted PIN block

3.1.6 The PAN must be masked when displayed (the first six and last four digits are the maximum number of digits that may be displayed)

3.1.7 The PAN must be rendered unreadable anywhere it is stored (including on portable media, backup media and in logs) by using any of the following approaches:

3.1.7.1 One-way hashes based on strong cryptography

3.1.7.2 Truncation

3.1.7.3 Index tokens and pads

3.1.8 Ensure that security policies and operation procedures for protecting stored cardholder data are documented, in use, and known to all affected parties

3.2 Encrypt transmission of cardholder data across open, public networks

3.2.1 Strong cryptography and security protocols such as SSH, TLS 1.2 or IPSEC must be used to safeguard sensitive cardholder data during transmission over open, public networks

3.2.1.1 Only trusted keys may be accepted

3.2.1.2 Protocol in use must only support secure versions or configurations

3.2.1.3 Proper encryption strength must be implemented for the encryption methodology in use

3.2.1.4 Wireless networks transmitting cardholder data or connected to the cardholder data environment must use industry best practices to implement strong encryption for authentication and transmission

3.2.2 Never send unprotected PANs by end-user messaging technologies (ex. Email, instant messaging)

3.2.3 Security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties

4.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214
Guideline: *PCI DSS Self-Assessment Questionnaire D v3.2*	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Syracuse University Information Technology Standard for PCI systems	http://its.syr.edu/security/standards/PCIstandard.pdf
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	Oct 01 2016
Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 25, 2017

Information Technology Standard for PCI systems
Syracuse University – Information Technology and Services
PCI – Vulnerability Management Standard (Appendix 3)

1.0 Scope

- All credit card data and its storage media.
- This includes any card holder data and card identifying information including names address of credit card holder.

Data which meets the guidelines above are considered to be *in scope* for the Payment Card Industry Data Security Standard (PCI DSS), and must confirm to the Credit Card Data Transaction and Storage Standard.

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS V 3.2 requirements for system components considered to be in scope as defined in Section 1.0 of this document.

3.0 PCI Network Security Standard

The standard below sets forth a set of requirements for the credit card data processing and storage in SU PCI Network. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaire D* and by the SU PCI Committee.

3.1 Protect all systems against malware and regularly update anti-virus software or programs

3.1.1 Anti-virus software must be deployed on all systems commonly affected by malicious software

3.1.1.1 All anti-virus programs must be capable of detecting, removing and protecting against all known types of malicious software

3.1.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software

3.1.2 Anti-virus software must be current, actively running, and generating audit logs, and logs are retained in accordance with PCI DSS Requirement 10.7

3.1.3 Anti-virus mechanisms must be actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period

3.1.4 Security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties

3.2 Develop and maintain secure systems and applications

3.2.1 A process must be established to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (include high and critical) to newly discovered security vulnerabilities

3.2.2 All system components and software (included payment application) must be protected from known vulnerabilities by having the latest vendor-supplied security patches installed

3.2.3 Software applications (internal and external, including web-based) must be developed in accordance with PCI DSS, ensuring the following:

3.2.3.1 Custom application accounts, user IDs and passwords are removed before applications become active or are released to customers

3.2.3.2 Custom application code changes are reviewed prior to release to production or customers in order to identify any potential coding vulnerability as follows:

3.2.3.2.1 Code changes are reviewed by individuals other than the originating code author and by individuals who are knowledgeable in code review techniques and secure coding practices

3.2.3.2.2 Code is developed according to secure coding guidelines (per PCI DSS Requirement 6.5)

3.2.3.2.3 Corrections are implemented prior to release

3.2.3.2.4 Code review results are reviewed and approved by management prior to release

3.2.4 Change control processes and procedures must be followed for all changes to system components to include the following:

3.2.4.1 Development/test environments are separate from the production environment with access control in place to enforce the separation

3.2.4.2 Separation of duties exists between personnel assigned to the development/test environments and those assigned to the production environment

3.2.4.3 Production data (live PANs) are not used for testing or development

3.2.4.4 Test data and accounts are removed before production systems become active

3.2.4.5 Change control procedures are documented for implementing security patches and software modifications and include:

3.2.4.5.1 Documentation of impact

3.2.4.5.2 Documented approval by authorized parties

3.2.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system

3.2.4.5.4 Back-out procedures for each change

3.2.5 Prevention of common coding vulnerabilities must be covered in software development processes to ensure that applications are not vulnerable to, at a minimum, the following:

3.2.5.1 Injection flaws such as SQL injection – also consider OS command injection, LDAP and XPath injection flaws

3.2.5.2 Buffer overflow Insecure cryptographic storage

3.2.5.3 Insecure communications

3.2.5.4 Improper error handling

3.2.5.5 All "high" vulnerabilities identified in the vulnerability identification process

3.2.5.6 Cross-site scripting (XSS)

3.2.5.7 Improper access control such as insecure direct object references, failure to restrict URL access, and directory traversal

3.2.5.8 Cross-site request forgery (CSRF)

3.2.5.9 Broken authentication and session management

3.2.6 Public-facing web applications must be protected against known attacks by applying either of the following methods:

3.2.6.1 Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:

3.2.6.1.1 At least annually

3.2.6.1.2 After any changes

3.2.6.1.3 By an organization that specializes in application security

3.2.6.1.4 That all vulnerabilities are corrected

3.2.6.1.5 That the application is re-evaluated after the corrections

3.2.6.2 OR install a web-application layer firewall in front of public-facing web applications to detect and prevent web-based attacks that is:

3.2.6.2.1 Up to date

3.2.6.2.2 Generating audit logs

3.2.6.2.3 Configured to either block web-based attacks or generate an alert

3.2.7 Security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties

Referred Documents, Web Pages and Contact Information

Item	Location/Info
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214
Guideline: *PCI DSS Self-Assessment Questionnaire D v3.2*	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Syracuse University Information Technology Standard for PCI systems	http://its.syr.edu/security/standards/PCIstandard.pdf
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	Oct 01 2016
Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 25, 2017

Information Technology Standard for PCI systems
Syracuse University – Information Technology and Services
PCI – Access Control Standard (Appendix 4)

1.0 Scope

- All credit card data and its storage media.
- This includes any card holder data and card identifying information including names address of credit card holder.

Data which meets the guidelines above are considered to be *in scope* for the Payment Card Industry Data Security Standard (PCI DSS), and must confirm to the Credit Card Data Transaction and Storage Standard.

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS V 3.2 requirements for system components considered to be in scope as defined in Section 1.0 of this document.

3.0 PCI Network Security Standard

The standard below sets forth a set of requirements for the credit card data processing and storage in SU PCI Network. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaire D* and by the SU PCI Committee.

- 3.1 Restrict access to cardholder data by business need to know
  - 3.1.1 Access to the system components and cardholder data must be limited to only those individuals whose jobs require such access, as follows:
    - 3.1.1.1 Define access needs for each role, including system components and data resources that each role needs to access for their job function, and level of privilege required for accessing resources
    - 3.1.1.2 Access rights for privileged user IDs are restricted to privileges necessary to perform job responsibilities
    - 3.1.1.3 Privileges are assigned to individuals based on job classification and function using role-based access control (RBAC)
    - 3.1.1.4 Documented approval by authorized parties is required to specify required privileges
  - 3.1.2 An access control system must be in place for systems to restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed, as follows:
    - 3.1.2.1 In place on all system components
    - 3.1.2.2 Configured to enforce privileges assigned to individuals based on job classification and function
    - 3.1.2.3 Default "deny all" setting
  - 3.1.3 Security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties
- 3.2 Identify and authenticate access to system components
  - 3.2.1 Proper user identification and authentication management controls must be in place for non-consumer users and administrators on all system components as follows:

3.2.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data

3.2.1.2 Control addition, deletion, and modification of user IDs, credentials and other identifier objects

3.2.1.3 Immediately revoke access for any terminated users

3.2.1.4 Remove/disable inactive user accounts at least every 90 days

3.2.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:

3.2.1.5.1 Enabled only during the time period needed and disabled when not in use

3.2.1.5.2 Monitored when in use

3.2.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts

3.2.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID

3.2.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session

3.2.2 Ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase
- Something you have such as a token device or smart card
- Something you are such as a biometric

3.2.2.1 Using strong cryptography, render all authentication credentials unreadable during transmission and storage on all system components

3.2.2.2 Verify user identity before modifying any authentication credential – for example, performing password resets, provisioning new tokens, or generating new keys

3.2.2.3 Passwords/phrases must meet the following:

3.2.2.3.1 Require a minimum length of at least seven characters

3.2.2.3.2 Contain both numeric and alphabetic characters

3.2.2.3.3 Alternatively, meet the complexity and strength requirements at least equivalent to the parameters specified above

3.2.2.4 Change user passwords/passphrases at least every 90 days

3.2.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used

3.2.2.6 Set passwords/phrases for first-time use and upon rest to a unique value for each user, and change immediately after the first use

3.2.3 Incorporate multi-factor authentication for all individual remote network access originating from outside the network by personnel (including users and administrators) and all third parties, including vendor access for support or maintenance for normal and non-console and non-console administrative access

3.2.4 Document and communicate authentication procedures and policies to all users including:

3.2.4.1 Guidance on selecting strong authentication credentials

3.2.4.2 Guidance for how users should protect their authentication credentials

3.2.4.3 Instructions not to reuse previously used passwords

3.2.4.4 Instructions to change passwords if there is any suspicion the password could be compromised

3.2.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed
- Shared user IDs do not exist for system administration and other critical functions
- Shared and generic user IDs are not used to administer any system components

3.2.5.1 Service providers with remove access to customer premises must use a unique authentication credential for each customer

3.2.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

3.2.6.1 Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts

3.2.6.2 Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access

3.2.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

3.2.7.1 All user access to, user queries of, and user actions on databases are through programmatic methods

3.2.7.2 Only database administrators have the ability to directly access or query databases

3.2.7.3 Application IDs for database applications can only be used by the applications, and not by individual users or other non-application processes

3.2.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties

3.3 Restrict physical access to cardholder data

3.3.1 Appropriate facility entry controls must be in place to limit and monitor physical access to systems in the cardholder data environment

3.3.1.1 Video cameras and/or access-control mechanisms must be in place to monitor individual physical access to sensitive areas

3.3.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks

3.3.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines

3.3.1.4 Data collected from video cameras and/or access control mechanisms must be reviewed and correlated with other entries, and data must be stored for at least three months unless otherwise restricted by law

3.3.2 Procedures must be developed to easily distinguish between onsite personnel and visitors including:

3.3.2.1 Identifying new onsite personnel or visitors

3.3.2.2 Changing access requirements

3.3.2.3 Revoking terminated onsite personnel and expired visitor badges

3.3.3 Control physical access for onsite personnel to the sensitive areas as follows:

3.3.3.1 Access must be authorized and based on individual job function

3.3.3.2 Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled

3.3.4 Implement procedures to identify and authorize visitors, including the following:

3.3.4.1 Visitors are authorized before entering areas where cardholder data is present

3.3.4.2 Visitors are given a physical token that visibly distinguishes visitors from onsite personnel

3.3.4.3 Visitors are asked to surrender the physical token before leaving the facility or upon expiration

3.3.4.4 A visitor log must be used to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted

3.3.4.4.1 The visitor log must contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and this information must be retained for at least three months

3.3.5 Physically secure all media related to cardholder data

3.3.5.1 Media backups must be stored in a secure location, preferably in an off-site facility such as an alternate or backup site, or a commercial storage facility - this location's security must be reviewed at least annually

3.3.6 Strict control must be maintained over the internal or external distribution of any kind of media

3.3.6.1 The media must be classified such that the sensitivity of the data may be determined

3.3.6.2 The media must be sent by courier or other delivery method that can be accurately tracked

3.3.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals)

3.3.7 Strict control must be maintained over the storage and accessibility of media

3.3.7.1 Inventory logs of all media must be properly maintained and be subject to periodic media inventories conducted at least annually

3.3.8 Media must be destroyed when it is no longer needed for business or legal reasons and destruction must be performed as follows:

3.3.8.1 Hardcopy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed

3.3.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed

3.3.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution

3.3.10 Maintain an up-to-date list of devices, including the following:

3.3.10.1 Make, model of device

3.3.10.2 Location of device

3.3.10.3 Serial number or other method of unique identification

3.3.11 Periodically inspect device surfaces to detect tampering (for example, card skimmers), or substitution (being swapped with a fraudulent device)

3.3.12 Provide training for personnel to be aware of attempted tampering or replacement of device, including the following:

3.3.12.1 Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices

3.3.12.2 Do not install, replace or return devices without verification

3.3.12.3 Be aware of suspicious behavior around devices

3.3.12.4 Report suspicious behavior and indications of device tampering or substitution to appropriate personnel

3.3.13 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties

Referred Documents, Web Pages and Contact Information

Item	Location/Info
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214
Guideline: *PCI DSS Self-Assessment Questionnaire D v3.2*	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Syracuse University Information Technology Standard for PCI systems	http://its.syr.edu/security/standards/PCIstandard.pdf
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	Oct 01 2016
Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 25, 2017

Information Technology Standard for PCI systems
Syracuse University – Information Technology and Services
PCI – Network Monitor Standard (Appendix 5)

1.0 Scope

- All credit card data and its storage media.
- This includes any card holder data and card identifying information including names address of credit card holder.

Data which meets the guidelines above are considered to be *in scope* for the Payment Card Industry Data Security Standard (PCI DSS), and must confirm to the Credit Card Data Transaction and Storage Standard.

2.0 Purpose

In order for Syracuse University to accept Credit Cards as a form of payment for any of its services, it must comply with the Payment Card Industry's Data Security Standard (PCI DSS). The purpose of this standard is to define the appropriate PCI DSS V 3.2 requirements for system components considered to be in scope as defined in Section 1.0 of this document.

3.0 PCI Network Security Standard

The standard below sets forth a set of requirements for the credit card data processing and storage in SU PCI Network. The requirements have been derived from the *Payment Card Industry Data Security Standard Self-Assessment Questionnaire D* and by the SU PCI Committee.

- 3.1 Monitor and test networks
  - 3.1.1 A process must be in place to link all access to system components to each individual user
  - 3.1.2 Automated audit trails must be implemented for all system components to reconstruct the following events:
    - 3.1.2.1 All individual user access to cardholder data
    - 3.1.2.2 All actions taken by any individual with root or administrative privileges
    - 3.1.2.3 Access to all audit trails
    - 3.1.2.4 Invalid logical access attempts
    - 3.1.2.5 Use of identification and authentication mechanisms – including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges
    - 3.1.2.6 Initialization of audit logs
    - 3.1.2.7 Creation and deletion of system-level objects
  - 3.1.3 Audit trail entries must be recorded for all system components for each event:
    - 3.1.3.1 User identification
    - 3.1.3.2 Type of event
    - 3.1.3.3 Date and time
    - 3.1.3.4 Success or failure indication
    - 3.1.3.5 Origination of event
    - 3.1.3.6 Identity or name of affected data, system component or resource
  - 3.1.4 All critical system clocks and times must be synchronized through use of time synchronization technology such as NTP, and the technology be kept current, including the following:
    - 3.1.4.1 Critical systems have the correct and consistent time

3.1.4.2 Time data must be protected

3.1.4.3 Time settings are received from industry-accepted time sources

3.1.5 Audit trails must be secured so they may not be altered, as follows:

3.1.5.1 Viewing of audit trails is limited to those with a job-related need

3.1.5.2 Audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation

3.1.5.3 Audit trail files are promptly backed up to a centralized log server or media that is difficult to alter

3.1.5.4 Logs for external-facing technologies (e.g., wireless, firewalls, DNS) are offloaded or copied onto a secure, centralized log server or media device on the internal LAN

3.1.5.5 File-integrity monitoring or change-detection software is used on logs to ensure that existing log data cannot be changed without generating alerts

3.1.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

3.1.6.1 Review the following at least daily:

3.1.6.1.1 All security events

3.1.6.1.2 Logs of all system components that store, process, or transmit CHD and/or SAD, that could impact the security of CHD and/or SAD

3.1.6.1.3 Logs of all critical system components

3.1.6.1.4 Logs of all servers and system components that perform security functions (firewalls, IDS, IPS)

3.1.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment

3.1.6.3 Follow up exceptions and anomalies identified during the review process

3.1.7 Log retention policies and procedures must be in place and require that audit trail history is retained for at least one year, with a minimum of three months immediately available for analysis

3.1.8 Ensure 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

3.2 Regularly test security systems and processes

3.2.1 A process to detect the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis

3.2.1.1 The methodology used must detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components
- Portable wireless devices connected to system components
- Wireless devices attached to a network port or network device

3.2.1.2 If automated monitoring is used, monitoring must be configured to generate alerts to personnel

3.2.2 Maintain an inventory of authorized wireless access points including a documented business justification

3.2.3 Implement incident response procedures in the event unauthorized wireless access points are detected

3.2.4 Internal and external vulnerability scans must be run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades) as follows:

3.2.4.1 Quarterly internal scan process includes rescans until passing results are obtained, or until all "High" vulnerabilities are resolved

3.2.4.2 External quarterly scan results satisfy the ASV Program Guide requirements

3.2.4.3 Perform internal and external scans and rescans as needed after any significant change. Scans must be performed by qualified personnel.

3.2.5 Implement a methodology for penetration testing that includes the following:

- Is based on industry-accepted penetration testing approaches
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threads and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results

3.2.5.1 Perform external penetration testing at least annually and after any significant infrastructure of application upgrade or modification (such as an OS upgrade, subnetwork addition, web server addition)

3.2.5.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification

3.2.5.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the connections

3.2.5.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests 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

3.2.6 Use intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines and signatures up to date.

3.2.7 Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly

3.2.7.1 Implement a process to respond to any alerts generated by the change-detection solution

3.2.8 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties

Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Standard: Payment Card Industry Data Security Standard V3.2	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1481746845214
Guideline: *PCI DSS Self-Assessment Questionnaire D v3.2*	https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1481747436821
Syracuse University Information Technology Standard for PCI systems	http://its.syr.edu/security/standards/PCIstandard.pdf
Contact:	Christopher Croad

Director of Information Security	ccroad@syr.edu

Document Info

Version:	3.0
Effective Date:	Oct 01 2016
Date of Last Review	October 25, 2016
Date of Next Mandatory Review	October 25, 2017