Version:	Modified By:	Date:	Approved By:	Date:
1.0	Michael Hawkins	October 29, 2013	Dan Bowden	November 2013

Rule 4-004L Payment Card Industry (PCI) Physical Security (proposed)

01.1 Purpose

The purpose of the Physical Security Rule is to ensure that information, systems and resources are safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats.

01.2 Scope

The Physical Security Rule addresses threats to information, systems and resources that arise from unauthorized access to the University of Utah ("University") facilities including offices, data centers and similar facilities.

01.3 Rule Statement

All information processing facilities shall be physically protected in proportion to the criticality or importance of their function. Physical access procedures shall be documented, and access to such facilities shall be controlled. Access lists shall be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

01.4 Security of Facilities

Area Statement: Access to information process facilities shall be controlled.

01.4.01 Securing Computing Facilities

Access to facilities dedicated to information processing (e.g., data centers, operations centers, media libraries, telecommunications rooms, UPS rooms, etc.) shall be physically restricted and access shall only be granted to those users, employees, and third-party consultants, contractors and vendors who have legitimate responsibilities in the facility. Any observed or reported incident of unauthorized access shall be reported immediately to the UIT Data Center Manager and Information Security Office. [Ref: CS078, PCI, HIPAA]

Access to facilities shall be authorized based on the frequency and length of time needed for an individual's roles and responsibilities. All requests for permanent access shall be approved by the manager responsible for the computing facility. [Ref: CS079, PCI, HIPAA]

The use of electronic access control systems shall be implemented to prevent unauthorized access to computer facilities. The system shall record all entries to the room and/or facility, and be capable of producing printed audit trails. [Ref: CS080, HIPAA]

Physical access audit logs shall be maintained in either electronic or printed form for at least two (2) months, be designated Restricted, and be provided security protection commensurate to that classification. Appropriate managers shall review these logs on a daily basis. [Ref: CS081, HIPAA]

Access to facilities that are dedicated to computer processing (e.g., data centers, computer rooms) shall be protected by a range of physical controls. Physical controls shall protect: [Ref: CS082, PCI, HIPAA]

- Buildings that house critical IT facilities against unauthorized access, by using locks, employing security guards and/or providing video surveillance
- Important papers and removable storage media such as CDs and diskettes against theft or copying, by complying with a ""clear desk"" rule, providing lock-out on unattended terminals, and restricting physical access to important post / fax points
- Easily portable computers and components against theft, by using physical locks and indelibly marking vulnerable equipment
- Employees against coercion from malicious third parties by providing duress alarms in susceptible public areas and establishing a process of responding to emergencies

In addition, the location of data centers shall not be identified or advertised by signage or other indicators.

All information processing facilities shall receive appropriate management approval, authorizing their purpose and use. Approval of the physical security designs shall also be obtained from the Information Security Office prior to utilizing the facility for processing to ensure the relevant security controls have been implemented. [Ref: CS475, PCI, HIPAA]

Health and safety practices shall be put in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations. [Ref: CS502, HIPAA]

All University data centers shall be protected through the coordinated use of trained personnel who have undergone the proper background checks and local law enforcement. [Ref: CS505, HIPAA]

Recordings / videos from cameras used to monitor sensitive areas of computing facilities shall be audited and correlated with other entries. Recordings shall be stored for a minimum of four months, unless otherwise restricted by law. [Ref: CS596, PCI]

01.4.02 Construction and Design

The following controls shall be implemented in relation to employees and visitor controls at University data centers: [Ref: CS491, PCI]

- A mantrap or optical turnstile shall be implemented. Design shall consider traffic flow for the proper number of these devices. Optical turnstiles are bi-directional; however,

recommended design is for two (2) on each side of reception station (i.e., entry on right, exit on left).

- A card read in and card read out system shall be implemented through employee controls. Attempt to pass through controls without proper card read will cause an alarm at security desk.
- All employee entrances other than main lobby shall contain a single person mantrap. Optical turnstile may be applied if staff is on 7X24 basis or when entry is in operation.
- Loading dock entry shall be controlled by security or other authorized personnel. These personnel shall be present at all times when entry door to dock or loading dock doors are open.

Main entry door will be of normal office entry design leading to a lobby where employees, visitors and vendors shall enter. If main entrance has multiple doors these controls may be applied to only one of those doors. All other doors may have standard locks. Entry doors shall be deactivated after hours when locked. Main entry will have the following: [Ref: CS492, PCI]

- Card reader on exterior for after hour employee entry, if required (7X24 staffing does not require)
- Door contact (if card reader applied)
- Electrified lock/strike (controlled by either central access system or security desk for after-hours entry control)

Network wiring requires some form of protection since it does not have to be physically penetrated for the data it carries to be revealed or contaminated. The following controls are recommended: [Ref: CS503, PCI]

- Using a conduit to encase wiring
- Avoid routing wiring through publicly accessible areas
- Avoid routing wiring in close proximity to power cables

The type of wiring to be used shall also be considered from a security point of view. For instance, signals over fiber are less susceptible to interception than signals over copper cable.

01.4.03 Physical Entry Controls

Doors used for access to computing facilities shall be locked at all times, and when feasible they shall be alarmed. The access cards or badges of individuals who only have temporary access authorization shall be collected prior to departure. [Ref: CS085, HIPAA]

Visitors to information processing facilities shall receive proper authorization, shall be provided a pass or badge to be displayed prominently, and provided escort as necessary. Visitors shall be asked to surrender the pass or badge before leaving the facility or at the date of expiration. [Ref: CS086, PCI]

All employees, third-party consultants, contractors and vendors are required to challenge and report individuals not displaying a correct access badge or are otherwise unknown. [Ref: CS087, PCI, HIPAA]

All employees, third-party consultants, contractors and vendors who do not require continued access to computing facilities in order to perform their job functions are to be considered visitors. [Ref: CS088, PCI, HIPAA]

Visitors shall be required to sign a visitor control log, and the Facility Manager shall maintain control logs for at least one (1) year. [CS089, PCI, HIPAA]

Badges shall be worn by all employees, contractors, third-party users and visitors and visible at all times while in sensitive University facilities. All employees, contractors, vendors and visitors shall immediately report any lost identification badges. [Ref: CS817, PCI]

Access rights to all facilities shall be reviewed on an annual basis. Access to areas deemed secure areas (e.g. computer data centers, security control centers, sensitive storage facilities or production processing centers), shall be reviewed on a quarterly basis**.** [Ref: CS818, PCI]

01.4.04 Securing Offices, Rooms and Facilities

Sensitive information resources shall be stored in rooms that can be secured when unattended, and shall not be located in areas accessible to the public or to unauthorized personnel. [Ref: CS090, HIPAA]

Office areas containing sensitive information resources shall be locked at the end of each business day. The recommended locking mechanism for room doors is automated. [Ref: CS091, HIPAA]

Intruder detection devices shall be implemented in all University data centers to prevent theft and safeguard equipment by alarming appropriate personnel when a response is necessary and to support subsequent forensics. [Ref: CS501, PCI, HIPAA]

[Rules] The following intruder detection devices shall be considered:

- Switches that activate an alarm when an electrical circuit is broken
- Light and laser beams, ultraviolet beams and sound or vibration detectors that are invisible to the intruder, and ultrasonic and radar devices that detect movement in a room
- Closed Circuit Television (“CCTV”) that allows observation and recording of actions

The following controls shall be considered to secure [sensitive] working areas: [CS092, HIPAA]

- Employees shall only be made aware of activities within a secured area on a need-to-know basis
- Sensitive materials shall be locked in secure cabinets immediately after use

- All desks and screens shall be cleared and workstations locked immediately after use
- Networked computers shall be password protected and have active screen savers
- Workstation activity shall be monitored to identify unauthorized access
- Unsupervised personnel working in secure areas shall be avoided to prevent malicious activities
- Third-party support services employees shall be granted restricted access to secure areas only when absolutely required
- Third-party access shall be authorized and monitored
- Photographic, video, audio or other recording equipment shall not be allowed

01.4.05 Working in Secure Areas

University personnel, third-party consultants, contractors and vendors are required to adhere to the following rules with respect to the disposal of information in hard copy form: [Ref: CS052, HIPAA]

- Disposal of Sensitive or Restricted information shall be disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Papers, slides, microfilm, microfiche and photographs containing sensitive information shall be disposed of by cross-shredding or burning.
- The use of third-party collection and disposal services for disposal of information in hard copy is authorized; however, care shall be exercised in selecting suitable contractors that exercise adequate security controls and have requisite experience. Background checks shall also be considered.
- Destruction of Restricted information shall be reported to the Information Owner in the form of a certificate of destruction which identifies when data was destroyed, who destroyed it, and means of destruction to permit them to update their records.

01.4.06 Health & Safety

The University shall compile a list of all service providers including data processing service providers, computing and communication providers, general utilities, heating, cooling, power and other providers that perform services or process data for the University and document all service provider related information. This includes: [Ref: CS800, PCI]

- Service provider contact
- All emergency service procedures
- Criticality and administrative units affected by the services
- Related contracts or service level agreements
- Security and controls reviews including any SSAE 16 or audit reports

01.5 Security of Information Systems

Area Statement: Access to workstations, laptops and handheld devices shall be controlled.

01.5.01 Workstation Protection

Access to workstations, laptops, and handheld devices that process sensitive information shall be limited by physical controls in addition to logical security controls. [Ref: CS095, PCI]

Systems processing highly sensitive data shall be physically isolated to reduce the opportunities for unauthorized access. This includes restricting physical access to network jacks, wireless access points and gateways at information processing facilities. [Ref: CS096, PCI, HIPAA]

Laptop computers shall not be left unattended or unsecured and shall be locked or secured when there is doubt of the security of the physical environment. Laptops shall not be checked in airline luggage systems, but remain in the possession of the traveler as hand luggage. [Ref: CS097, HIPAA]

Cabling and line facilities supporting voice and data communications shall be protected with controls consistent with requirements for physical and environmental controls such as alternative power supplies, physical access and environmental management facilities. [CS099, PCI]

[Rules] Physical and environmental controls to protect cabling and line facilities include:

- Voice networks shall be protected with controls to ensure availability of service and security of communications.
- To minimize the threat of interception or damage, all cable and line facilities for both voice and data shall be secured. Consideration shall be given to the use of shielding, conduit, burial and routing away from uncontrolled areas to meet this requirement.
- In-house telephone exchanges shall have the capacity to cope with peak workloads and expansion / upgrade capabilities to cope with projected demand.
- Monitoring of voice and data networks shall include monitoring facility capable of providing reports on usage, traffic and response statistics.
- In-house telephone exchanges shall be supported by continuity controls such as duplicate processors and function cards, emergency bypass, duplicate groups of exchange lines, access to alternative main exchanges operated by service providers and a source of power capable of coping with prolonged power failures. Additionally, voice and data systems shall be accounted for in all contingency and business continuity plans.
- Timely repair shall be ensured by the use of maintenance contracts providing agreed response times for in-house telephone exchanges and operator consoles, and for telephone and associated wiring / cables.

- Identification labels shall be attacked to communications equipment and cables.

01.5.02 Network / Server Equipment

All information resources classified as network equipment (e.g., LAN servers, routers, hubs, modem banks, etc.) shall be located in a secured facility. If possible, it will be housed in a dedicated computer room or data center. If this is not possible, such equipment will be secured in locked rooms, such as the telephone or wiring closets. [Ref: CS103, PCI]

01.5.03 Equipment Maintenance

A record of all maintenance activities will be maintained and will include the date, incident, modifications and name of the person or persons making the modifications. [Ref: CS107, HIPAA]

All transfers, loss, replacement or other physical movement of hardware will be reported according to established procedures within each administrative unit. [Ref: CS108, HIPAA]

All Sensitive or Restricted information shall be purged through overwrites prior to hardware being released for off-site maintenance. [Ref: CS109, HIPAA]

01.5.04 Security of Equipment Off-Premises

The following rules shall be considered when protecting off-site equipment: [Ref: CS112, HIPAA]

- Equipment and media taken off the premises shall not be left unattended in public places
- Portable computers shall be carried as hand luggage when traveling
- Manufacturer's instructions for protecting equipment shall be observed at all times
- Home office controls shall be determined by a risk assessment and suitable controls applied as appropriate (e.g., lockable filing cabinets, ""clear desk"" policy, access controls on personal computers, etc.)
- Adequate insurance coverage shall be in place to protect off-site equipment

01.5.05 Secure Disposal or Re-Use of Equipment

All equipment containing storage media (e.g., fixed hard disks, tapes, diskettes) shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. If it cannot be sanitized it shall be destroyed or kept unless an exception is granted by the appropriate official. [Ref: CS113, PCI, HIPAA]

Damaged storage devices containing sensitive data require a risk assessment to determine if the items shall be destroyed, repaired or discarded. [Ref: CS114, HIPAA]

01.5.06 Removal of Equipment

Inventories of University resources shall be maintained and spot checks shall be performed to detect unauthorized removal of property. Employees, third-party consultants, contractors and vendors shall be advised that spot checks will take place. [Ref: CS116, HIPAA]

01.5.07 Unused Ports and Cables

Procedures for controlling physical and logical access to diagnostic and configuration ports shall be established. Access ports that no longer support authorized connections shall be disconnected and unused cables shall be removed from network components. [Ref: CS119, PCI]

01.6 Fire Protection

Area Statement: Fire protection controls shall be implemented.

01.6.01 Monitoring Systems

Facility managers shall develop procedures for monitoring and responding to fire incidents. [Ref: CS133, HIPAA]

01.7 Contacts

A. Policy Owner: Questions about this Rule should be directed to the CISO, 801-213-3397 IT_policy@utah.edu
B. Policy Officer: Only the CIO, 801-581-3100, has the authority to grant exceptions to this Rule.

01.8 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C. Data Classification Model

01.9 Policy Meta-Data

A. Policy Owner
B. Audience
C. Status
D. Published Date
E. Effective Date
F. Next Review Date

01.10 Revision History