THE
UNIVERSITY
OF UTAH

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

Rule 4-004H Payment Card Industry (PCI) Secure Communications Management (proposed)

01.1 Purpose

The purpose of the Communications Management Rule is to ensure proper procedures and controls are in place to protect the confidentiality, integrity and availability of PCI data transmitted over and stored on the University of Utah (“University”)’s networks.

01.2 Scope

The Communications Management Rule applies to all PCI systems, resources and networks connected to the University’s networks.

01.3 Rule Statement

University Information Technology (“UIT”) and Information Security shall implement a communications management program with operating procedures and technical controls to ensure the secure transmission of PCI data over the University’s networks.

01.4 Encryption of PCI Systems

01.4.01 Use of Encryption

Encryption shall be employed to protect the confidentiality of information when being transmitted or stored on the University’s information resources. The appropriate method of encryption shall be implemented based on the classification of the data and method of storage and transmission: [Ref: CS241, PCI, HIPAA]

[Rules] The following rules shall be followed when transmitting information:

- **Public** - No requirement
- **Internal Use Only** - Encryption is recommended for transmission over network links containing equipment that is not owned or controlled by the University
- **Sensitive** - Encryption shall be used for transmission over network links containing equipment that is not owned or controlled by the University. It is recommended that transmissions over the University's network also be encrypted if available.
- **Restricted** - Encrypt using communication protocols with strong encryption such as SSL, Point-to-Point Tunneling Protocol (PPTP) or Internet Protocol Security (IPSEC).

[Rules] The following rules shall be followed when storing information:

- **Public** - No requirement
- **Internal Use** - No requirement
- **Sensitive** - Encrypt for storage on any information resource using strong encryption, unless the resource has user authentication, access controls and time outs
- **Restricted** - Encrypt using an algorithm for encryption that has been validated and approved for use within the organization

01.4.02 Key Management

Encryption key owners are responsible for the protection and management of public and private encryption keys entrusted to them and shall adhere to the following standards: [Ref: CS248, PCI]

- Key owners may not print out private keys and shall password-protect User IDs that contain each user's encryption keys
- Private keys shall be transmitted through different channels to ensure proper separation from the information which is used to generate the encryption keys
- All encryption systems shall be protected with appropriate security controls
- Private keys shall be classified at the same level as the information being encrypted
- Access to private keys shall be managed on a need-to-know basis
- Private keys may not be revealed to third parties without the approval of the Information Security Office. Note: Public keys may be shared in a public directory
- Private keys shall be managed via split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

To protect against potential compromise, encryption keys shall expire and be renewed periodically. The maximum time allowed between changes depends on the key type. [Ref: CS250, PCI]

[Rules] The following rules shall be used to determine maximum time to renew encryption keys:

- Keys used for transmission - per message or per session (e.g., maximum session time shall be limited to twenty-four (24) hours)
- Private Keys - two (2) years

- Keys for stored data - two (2) years. This may be granted exceptions based on backup system capabilities
- Keys used for encryption or cardholder data - annually

Procedures shall be in place to change an encryption key when it has been compromised. [Ref: CS251, PCI]

All hardware housing key management applications or used for generation of encryption keys shall be protected at the highest level of security controls. [Ref: CS840, PCI]

01.5 Exchange of Information

01.5.01 Information Exchange Agreements

Formal information exchange agreements shall be executed when exchanging information between the University and external organizations. The security content of such agreements shall reflect the sensitivity of the information involved. [Ref: CS253, PCI, HIPAA]

[Rules] Information Exchange Agreements shall document the following:

- Management responsibilities for controlling transmission, dispatch and receipt
- Procedures for notifying sender of transmission, dispatch and receipt
- Minimum technical standards for packing and transmission
- Courier identification standards
- Responsibilities and liabilities in the event data is lost
- Use of an "agreed upon" labeling system for classified information
- Ownership and responsibilities for data protection and copyright compliance issues
- Technical standards for recording and reading information and software
- Any special controls that may be required to protect sensitive items, such as encryption keys

01.6 Email, Internet and Other Electronic Communications

01.6.01 Use of Encryption

Information classified as Restricted or Sensitive shall not be sent over the Internet (e.g., email, ftp), via Remote Access or other external networks unless the message is using an encryption service approved by Information Security. The approved services can be access by contacting the CISO. [Ref: CS261, PCI, HIPAA]

[Rules] Examples of information that shall be encrypted include:

- Credit card numbers or other cardholder information
- Protected Health Information (“PHI”)
- Passwords
- Research and development information
- Employee social security numbers
- Employee healthcare-related information

01.7 Voice / Fax / Video Communications

01.7.01 Voice Mail

Where telephone systems are used to transmit or store Restricted or Sensitive information (e.g., conference calls and recorded telephone conversations), the media used to store or transmit this shall be subject to access controls. Employees shall not leave sensitive messages on any type of telephone answering machines. [Ref: CS842, PCI, HIPAA]

01.8 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.

01.9 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C. Policy 4-010: Information Security Management Policy
D. Data Classification Model

01.10 Policy Meta-Data

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

01.11 Revision History