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

Rule 4-004G Payment Card Industry (PCI) Remote and Mobile Access Security (proposed)

01.1 Purpose

The purpose of the Remote and Mobile Access Rule is to provide rules to provision and use remote and mobile devices supporting PCI systems in accordance with practices that:

- Meet the University of Utah's ("University") business requirements
- Protect the University's PCI systems and resources against attacks that exploit remote and mobile transmissions
- Prevent unauthorized remote and mobile device deployments
- Enable remote and mobile technologies that meet the University's security requirements

01.2 Scope

The Remote and Mobile Access Rule applies to all PCI systems, resources and networks connected to the University's network.

01.3 Rule Statement

The Information Security Office shall implement a remote and mobile access program to manage the use of remote and mobile devices to access the University's PCI systems, resources and networks.

01.4 Remote Access for PCI Systems

Area Statement: All remote and mobile devices connected to the University's network shall be approved by the Information Security Office and use approved protocols and configuration standards.

01.4.01 Requesting / Granting Access

Remote access to the University's information systems and resources is disallowed, unless a valid business justification exists and has been approved by the requesting user's manager. The approved request shall remain on file with the appropriate resource administrator as long as the individual has access. [Ref: CS340]

Remote access accounts granted to third party personnel (consultants, contractors or vendors) shall be assigned an owner, who should be an employee of the University. [Ref: CS341]

01.4.02 Remote Computing Devices

All external connections to University’s PCI information systems and resources require strong two-factor authentication. [Ref: CS342]

Third-party personnel accessing the University's network shall be limited so they can only access the information resources which they are authorized to access. In addition, the following controls are recommended:

- File access limitations
- Time limits for access, based on need
- Third party user accounts shall automatically expire on a specified date

Technologies such as Remote Authentication Dial-In User Service (“RADIUS”) or Terminal Access Controller Access Control System (“TACACS”) with tokens, or VPN with individual certificates shall be used.

Remote access to University resources shall be managed through approved access control points such as a centralized remote access solution (“VPN”), Microsoft Lync, remote meeting/collaboration solutions approved by the PCI system owner, or managed modem/dial in point. [Ref: CS578, PCI]

This Rule applies to all telecommuting environments processing University PCI even when the equipment being used is privately owned by the individual. Controls for limiting the time of access and the information allowed to be processed in the telecommuting environment shall be established based on the business requirements. Insurance, support and maintenance requirements shall also be defined for all telecommuting environments. The University shall provide suitable equipment and security controls for all approved telecommuting environments where privately owned equipment is not allowed or does not meet security requirements. Approval for telecommuting environments shall only be granted if appropriate security controls are implemented in the environment. [Ref: CS841, PCI]

Security controls for telecommuting environments shall comply with the University’s information security policies. Security controls to guard against theft, unauthorized disclosure and unauthorized access shall ensure that telecommuting environments:

- Are assessed for meeting logical and physical security requirements
- Meet communications security requirements; prevent access to unauthorized persons
- Do not cause disputes concerning intellectual property rights for information developed on privately owned equipment
- Do not prevent access to privately owned equipment in the event of an investigation by legislation
- Do not bind the University to privately owned software agreement obligations and liabilities

- Are properly firewalled and protected against malicious code attacks.

Users who work with University information in a home office shall understand what security threats exist in their home office environment and take appropriate measures to ensure the security of the information in that environment.

01.4.03 Mobile Devices

Mobile computing devices shall be configured based on the University's standard for the device. The baseline configuration shall include settings to comply with the University's standards for security controls such as passwords, session timeouts, data privacy, protection against malicious code and usage of mobile code. Where possible, configuration settings shall be pushed to mobile devices from a centralized management server to ensure proper configuration. In cases where this is not feasible, a configuration guide shall be provided to all employees that are using University issued mobile devices to ensure proper configuration. [Ref: CS098, HIPAA]

All computers and mobile devices used for University business or storage of University information shall employ encryption for all information that is classified as Sensitive or Restricted as defined in Information Security Policy 4-004.

01.4.04 Remote Control Software

Remote control software systems shall be limited to authorized technical support personnel that need to use remote support software as part of their job function. [Ref: CS343]

Remote control software shall not be installed on user workstations except to support the remote administration of approved servers by resource administrators. [Ref: CS344]

Requests to install remote control software on workstations shall be forwarded to the Information Security Office and be accompanied by a justification stating: [Ref: CS345]

- The intended use
- The machine where this shall be used
- A justification as to why alternate support methods cannot be used

01.4.05 Modem Connections

Information resources that are connected to the University's network shall not be connected to modems, unless a compelling business justification exists and the use of a modem has been approved by the Information Security Office. [Ref: CS346]

Modem connections that have been approved by the Information Security Office and information resources that are stand-alone, without any bridge or connection to the University's networks, may use modems. The following controls shall be implemented to protect against unauthorized modem connections:

- Dial-back features shall be enabled
- Call forwarding features shall be disabled
- Modem shall not answer inbound calls if they are for outbound use only
- Modem shall be disabled or unplugged by default and only enabled during the time it is needed
- Two-factor authentication shall be used (e.g., PIN-based token card with a onetime random password)
- The date, time, user, user location, duration and purpose for the use of the modem shall be documented
- If administrative-related procedures are being performed, all transactions shall be encrypted
- When accessing cardholder data remotely via modem, the following shall be disabled:
    - Storage of cardholder data onto local hard drives, floppy disks or other external media
    - Cut, paste, and print functions

If long-term access is needed, a modem bank or Remote Access Server ("RAS") shall be implemented to centralize modem and Internet access, to provide a consistent authentication process, and to subject inbound and outbound traffic to firewall controls.

01.4.06 Third Party Access

When an external connection to the University's PCI systems is granted, detailed instructions shall be provided to the recipient. These instructions shall notify the recipient of any security requirements, which include the need to maintain the confidentiality of the information, requirements for distribution of the information within their organization, and procedures for the destruction or return of the information following the period of access. [Ref: CS339]

01.4.07 Remote Logins

The following standards for remote logins are applicable to untrusted relations firewall systems: [Ref: CS371, PCI]

- Incoming remote logins (e.g., Telnet, rlogin) shall be treated as external connections and require approval
- Outgoing remote logins (e.g., to an external server) are to be handled in accordance with the University's information security policies

01.5 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.

01.6 References

A. Policy 4-002: Information Resources Policy

B. Policy 4-004: University of Utah Information Security Policy

C.

01.7 Policy Meta-Data

A. Policy Owner

B. Audience

C. Status

D. Published Date

E. Effective Date

F. Next Review Date

01.8 Revision History