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

Rule 4-004F Payment Card Industry Wireless Access Security (proposed)

01.1 Purpose

The purpose of the Wireless Access Security Rule is to provide guidelines to provision and use wireless networks 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 Wireless 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 wireless access program to manage the installation and access to wireless access points involved with processing, transmitting, or storing PCI connected to the University's network.

01.4 Wireless Access Rule

Area Statement: All wireless access points and devices supporting PCI systems connected to the University's network shall be approved by the Information Security Office and use approved protocols and configuration standards.

As of February 2014, there is NO APPROVED USAGE of any wireless (wifi) system for PCI

01.5.01 Wireless Access Restrictions

All wireless access points shall be approved by a UIT Financial Controller representative, the Network Operations Manager and a representative from the Information Security Office. Wireless access points shall be registered with the Network Operations Team, in the Point-of-Contact (POC) database. [Ref: CS579, PCI]

01.5.02 Configuration

Authentication and network/transport layer encryption shall be used for wireless connections to protect wireless access to the information system. Extensible Authentication Protocol ("EAP") with Wi-Fi Protected Access (WPA or WPA2) or IEEE 802.11i, IPSEC VPN or SSL/TLS are the recommended methodologies.

If one of the above methodologies cannot be used, the Information Security Office shall perform a risk assessment and determine appropriate security requirements and/or mitigating controls such as a hardware upgrade or intrusion detection systems.

01.5.03 Access Control

Access to wireless access points shall be limited and the administrator shall document and track the number or profiles of authorized users.

Physical access controls shall be employed to restrict unauthorized personnel and prevent the removal or unauthorized modification of wireless devices installed in a University facility.

All wireless network devices such as Wireless Intrusion Detection Systems ("WIDS") and wireless routers, access points, gateways, and controllers shall be located in a secure room with limited access to prevent tampering or theft.

01.5.04 Asset Management

A list shall be maintained of all wireless access points and devices. The following types of information should be maintained:

- Access point Media Access Control ("MAC") address
- Access point IP address
- Wireless client MAC address
- Network DHCP range
- Type of encryption enabled
- Access point Service Set Identifier ("SSID")
- Manufacturer, model number, and serial number of wireless equipment
- Equipment location
- Assigned users with telephone numbers
- An assessment shall be conducted at least quarterly to verify standard configurations and validate that un-authorized access points do not exist PCI processing infrastructure locations.

01.6 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.

01.7 References

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

01.8 Policy Meta-Data

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

01.9 Revision History