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

Rule 4-004E Payment Card Industry (PCI) Network Security (proposed)

01.1 Purpose

The purpose of this Network Security Rule is to ensure the effective management, operation, integrity and security of the University of Utah (“University”)’s information systems and networks involved with storing, processing, or transmitting PCI information.

01.2 Scope

The Network Security Rule applies to all information systems, resources and networks connected to the University’s network which store, process, or transmit PCI.

01.3 Rule Statement

University Information Technology (“UIT”) and Information Security shall implement a network security program with network operating procedures and technical controls to manage the design, implementation and maintenance of the University’s PCI technology infrastructure.

01.4 Network Access for PCI Systems

01.4.01 Use of Network Services

Well-defined controls and/or processes shall be followed when granting access to the University's network services. [Ref: CS348, PCI]

[Rules] The following controls and/or processes shall be followed when granting access to the University's network services:

- Connections shall be authorized by the Information Security Office and Income Accounting for PCI.
- Any remote support services offered by the network service providers shall comply with University and/or PCI standards with regard to remote vendor support
- All network services shall pass through the University's firewall which will only allow the defined protocols and services required to provide the functionality
- The functionality of defined protocols and ports shall be analyzed as part of the risk assessment effort during the initial firewall setup. Justification and documentation shall be captured for allowed risky protocols including reason for use and security features

implemented. (Use of protocols offering a high degree of functionality that may pose a risk to the University's systems shall also be identified in the Risk Assessment Process)

- Appropriate controls shall be put in place on the University's side of the network to minimize the risk of unauthorized access or activity within PCI systems.
- When possible, the connection shall be initiated by the internal client to the network service supplier
- Ensure that proper agreements are in place with information suppliers and held by Income Accounting, the Privacy Office and the Office of General Counsel.
- Firewalls will log and monitor all unauthorized activity

Network services provided by third parties may have unique, complex security characteristics. Administrative units leveraging these network services shall request detailed documentation on the security attributes of all network services provided by third parties. [Ref: CS359]

01.4.02 Inventory of Network Access Points

All access points to the University's network shall be identified and documented by [UIT]. [Ref: CS350, PCI]

[Rules] Network access points that shall be identified include:

- Wireless
- Ethernet
- Frame relay
- Dedicated lines
- Remote dial-up access
- Extranets
- Internet

[UIT] shall also identify and document the applications and user groups that are accessed via the network and map the internal and external connectivity between various network segments. The information shall be used by UIT in the design, configuration and maintenance of the University's network.

01.4.03 Remote Diagnostic Ports

Remote maintenance ports for the University's information and communication resources shall be disabled until the specific time they are needed by a vendor who has received prior authorization by University personnel. Audit logs shall be reviewed for all remote maintenance sessions and ports shall be disabled immediately after use. [Ref: CS351, PCI]

An information system security plan shall address the installation and use of remote diagnostic links. [Ref: CS582]

01.4.04 Network Segregation

Networks shall be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices. [Ref: CS352]

Switched network technology shall be utilized when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic. A firewall shall be installed at all connections from an internal to any other internal or external network. [Ref: CS353]

Servers which access external networks or are accessed from external networks shall be logically isolated from the private Intranet. [Ref: CS354]

01.4.05 Network Connections

The Information Security Office shall explicitly authorize all new connections to external public networks (e.g. extranets). If the new connection is an additional connection to a previously certified external connection, and the connection is made following the same configuration, then no prior approval from the Information Security Office is required. [Ref: CS355]

All external access from untrusted systems or networks (e.g. extranets) to any University network shall be controlled through the implementation of an approved firewall. A listing of approved firewall products can be accessed by contacting the Direction of Common Infrastructure Services [Ref: CS363, PCI]

Personal computers, workstations, and servers shall not be connected to more than one network at a time by using unauthorized means of bridging two networks. This may include inserting more than one Network Interface Card (NIC) or using a modem while connected to another network. Dual-homed systems require approval by the Information Security Office. [Ref: CS512]

Denial of Service (“DoS”) attacks are actions that are designed to prevent or impair the use of networks, systems or applications by stressing system resources such as processing units or network bandwidth. The University shall implement specific controls to prevent DoS attacks. [Ref: CS879]

[Rules] The following controls shall be implemented to prevent DoS attacks:

- The [technical manager] responsible for [network management] shall establish communication protocols and prevention and response procedures with all Internet Service Providers (“ISPs”) in the case of a DoS attack.
- Intrusion detection devices deployed shall be configured to specifically identify possible DoS situations.
- Network management procedures shall be in place to monitor network bandwidth and usage and alert when thresholds indicate a potential issue.

- Network devices connected to public networks shall be configured specifically to prevent DoS attacks including:
    - Blocking the usage of services, such as echo and chargen, which no longer serve a legitimate purpose and are used in DoS attacks.
    - Performing egress and ingress filtering to block obviously spoofed packets.
    - Blocking traffic from unassigned IP address ranges, known as bogon lists.
    - Attack tools that spoof IP addresses may use addresses that have not yet been assigned for Internet usage.
- Writing and sequencing firewall rules and router access control lists to block traffic properly.
- Configuring border routers not to forward directed broadcasts.
- Limiting incoming and outgoing ICMP traffic to only the necessary types and codes.
- Blocking outgoing connections to common IRC, peer-to-peer service and instant messaging ports if the usage of such services is not permitted.

[Rules] The University shall define specific procedures to respond to a DoS attack including:

- Protocols to notify and work with Internet Service Providers.
- Backup copies of critical information (procedures, call lists, etc.) that may not be accessible due to the DoS attack.
- Containment strategies or procedures for common scenarios of DoS attacks.
- Evidential procedures for the collection of data in the case of a possible criminal attack.

01.4.06 Network Routing

Shared networks that extend across organizational boundaries shall incorporate routing controls to ensure computer connections and information do not breach the access controls of the application. [Ref: CS356, PCI]

Routing controls shall be based on a positive source and destination address-checking mechanism. Only authorized University resource administrators shall be allowed to have physical and logical access to network routers. [Ref: CS357]

Proprietary routing information pertaining to the private Intranet shall not be propagated to any untrusted network. [Ref: CS358]

[Rules] The following proprietary routing information shall not be propagated to any untrusted network:

- Routing tables
- Domain Name Service (“DNS”) names
- IP addresses
- Network Address Translation (“NAT”) tables
- Access Control Lists (“ACLs”)

01.4.07 Limitation of Connection Time

For applications that support information classified as Restricted or Sensitive, resource administrators shall consider placing restrictions on the connection times during which connections are allowed to computer services, thus reducing the window of opportunity for unauthorized access. Limiting connection times is especially important for information resources that are located in public or external areas that are outside the University's domain of control [management]. [Ref: CS471]

01.5 Network Security Control Devices for PCI Systems

01.5.01 Use of Firewalls

All external access from untrusted systems or networks (e.g. extranets) to any University network shall be controlled through the implementation of an approved firewall. A listing of approved firewall products can be accessed by contacting the Director of Common Infrastructure Services [Ref: CS363, PCI]

All rules within the firewall rule base shall be restricted to only allow the appropriate traffic through the firewall. All rules defined within the firewall shall be documented with a clear description and definition for the business purpose of the rule. Firewall/router rule sets shall be reviewed quarterly. [Ref: CS364, PCI]

[Rules] The firewall rule base shall:

- Restrict source and destination IP addresses, protocols, ports and applications (e.g. outbound traffic from payment card applications shall be restricted to Internet Protocol (IP) addresses within the Demilitarized Zone (“DMZ”)).
- Be configured to deny and log suspicious packets (e.g. packets that have suspicious source and destination ports).

In the event a firewall fails, and a standby firewall is used, all active sessions on the firewall shall be re-authenticated on the standby firewall. [Ref: CS477]

The Information Security Office shall be responsible for creating and maintaining the University's Firewall Management Procedures. The Firewall Management Procedures shall state describe how firewalls shall function by establishing rules for traffic coming into and going out of the security domain, and for how the firewall will be managed and updated. [Ref: CS500, PCI]

[Rules] The Firewall Management Procedures shall address:

- Firewall topology and architecture (include application firewalls in front of web-facing applications)
- Type of firewall(s) being used
- Physical placement to the firewall components
- Monitoring of firewall traffic
- Permissible traffic (generally based on the premise that all traffic not expressly allowed is denied, detailing which applications can traverse the firewall and under what exact circumstances such activities can take place)
- Firewall updating
- Coordination with intrusion detection and response mechanisms
- Responsibility for monitoring and enforcing the Firewall Policy
- Description of groups, roles, and responsibilities for logical management of network components
- Protocols and applications permitted
- Regular auditing of a firewall's configuration and testing of the firewall's effectiveness
- Contingency planning
- Placement of firewalls within the network architecture including on all connections to public networks and between internal systems and perimeter devices such as wireless access points or dial-in points

01.5.02 Use of Demilitarized Zones (DMZs)

The University's Internet servers shall always be placed in a DMZ. By placing Internet servers and any other servers in the DMZ, the University can reduce the potential risk of unauthorized access to its information resources. [Ref: CS356, PCI]

Intrusion Detection Software shall be implemented inside all DMZs to monitor the firewall and to monitor communications allowed through the firewall. [Ref: CS366, PCI]

01.5.03 Packet Filter Configuration

Well-defined configuration standards shall be applied to packet filters. [Ref: CS367, PCI]

[Rules] The following standards shall be applied in relation to packet filters:

- Configuration and control of the packet filters shall be assumed internally and shall only be possible from an internal interface
- All privileged ports, with the exception of explicitly required ports, shall be closed
- All incoming traffic to non-privileged ports, except for acknowledgement packets, shall be rejected. External packets with an internal source IP address shall be identified and rejected, and an attacker alarm shall be triggered
- Internal packets with an external source IP address shall be identified and rejected, and an attacker alarm shall be triggered
- Attacker alarms are defined as a notification sent via email or pager to support personnel

01.5.04 Router Configuration

Well-defined router configuration standards shall be followed when configuring routers. The router configuration files shall be backed up and secured. [Ref: CS368, PCI]

[Rules] The following configuration standards shall be followed when configuring routers:

- Source routing shall be switched off on the router
- External OSPF, RIP or other routing information protocols shall be blocked
- Amongst the ICMP protocols, only ping may be accepted
- The TFTP protocol shall be blocked
- SNMP traffic may only be accepted by administration workstations and shall not accept a public string
- At a minimum, the router shall log rejected packets
- Remote access to the router requires strong authentication
- Remote access to the router shall be limited to internal workstations
- Remote access to the router shall be limited to a static IP address
- Each administrator shall be identified with a personal User ID
- All changes shall be documented
- IPv6 should be disabled unless it is approved by the Director of Common Infrastructure Services

- Running and startup configuration files shall be synchronized

01.5.05 Host Configuration

The configuration of the firewall operating system shall follow well-defined security requirements in addition to the relevant baseline security configuration standard (e.g. UNIX, NT, etc.). [Ref: CS369]

[Rules] The configuration of the firewall operating system shall satisfy the following requirements:

- Packet forwarding shall be switched off
- Remote access to the host can only be permitted from specific internal hosts and requires strong authentication
- Each administrator shall be identified with a personal User ID
- All unnecessary network services shall be switched off The "Berkeley r" protocols shall be blocked
- NFS shall not be used
- Neither compilers nor debuggers can be installed
- All changes shall be documented
- The operating system error mode shall be set in such a manner that packets cannot pass through if the firewall software crashes
- The firewall software shall be started before the interfaces
- Apart from the administrators, no user is permitted to access the firewall computer
- It shall be ensured that vendor security patches are installed
- Regular basis integrity checks (e.g. at least once a day) shall be completed

01.5.06 File Transfer Protocol (FTP)

Configuration standards shall be defined for File Transfer Protocols (“FTP”) used with untrusted systems. [Ref: CS372]

[Rules] The following standards for FTP are applicable to use with untrusted systems:

- Incoming file transfers shall be treated as external connections and require approval
- Incoming anonymous file transfer is not permitted
- FTP configuration shall implement controls for protecting data channels

- Outgoing file transfers (e.g. to an external server) are to be handled in accordance with the University's Internet Security Policy

01.5.07 Hyper Text Transfer Protocol (HTTP)

Configuration standards shall be defined for HTTP used with untrusted systems. [Ref: CS373]

[Rules] The following standards for HTTP are applicable to use with untrusted systems:

- Port 80 shall be blocked against external access
- Alternative ports such as 8080 shall be protected against external access
- All HTTP servers that can be accessed externally shall be in a DMZ
- Proxying and/or stateful inspection shall be used for all connections to and from the public Internet and other untrusted networks
- Rules of the University's Internet Security Policy apply when accessing internal objects

01.5.8 Non-Essential Services

Configuration standards shall be defined for services used with untrusted systems. [Ref: CS376]

[Rules] The following standards are applicable to services used with untrusted systems:

- All non-IP protocols shall be blocked by the firewall. SNMP traffic shall be blocked in both directions
- NTP traffic is only permitted to a central, internal timeserver
- The use of "Berkeley r" protocols by the firewall is generally forbidden
- The firewall shall prevent the following protocols from entering:
  - NFS
  - RPC portmapper
  - NIS
  - TFTP
  - X11
  - Finger
- UDP packets are only permitted in conjunction with a "status-creating" proxy

- All unused network services (e.g. Telnet) and unnecessary shells and interpreters (e.g. Perl) shall be disabled on all WWW host machines.

01.5.9 Domain Name Server

Configuration standards shall be defined for DNS used with untrusted systems. [Ref: CS378]

[Rules] The following DNS standards are applicable to use with untrusted systems:

- Internal host names and IP addresses are classified as "internal" and shall not be visible externally
- Queries to non-existent host names shall be logged and rejected
- A split DNS configuration shall be used
- External DNS entries are limited to servers externally accessible
- No queries may be forwarded to internal DNS services from external DNS services

01.5.10 Requirements for Network Traffic Filtering

Filtering of network traffic to control and restrict access across the University's network perimeter shall be utilized. [Ref: CS382, PCI]

[Rules] This filtering of network traffic shall include:

- Destination and source IP addresses
- Ports
- Applications
- Protocols
- Any non-business justified traffic that is prohibited by the University's information security policies.

01.5.11 Proprietary Routing Information

Methods shall be utilized to prevent proprietary routing information from being propagated. [Ref: CS383, PCI]

[Rules] Methods to obscure proprietary routing information may include:

- Network Address Translation (“NAT”)
- Placing servers containing cardholder data behind proxy servers/firewalls or content caches

- Removal or filtering of route advertisements for private networks that employ registered addressing
- Internal use of RFC1918 address space instead of registered addresses

01.6 Contacts

A. Rule 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