## Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Prepared By</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft version 1.0</td>
<td>22-Mar-13</td>
<td>Credit Card Acceptance Committee</td>
<td>Revised the Firewall Configuration Standards to include other network devices including routers and switches. This new Network Device Configuration Standard will replace the Firewall Configuration Standard and the Router Configuration Standard.</td>
</tr>
<tr>
<td>Final Version 1.2</td>
<td>09-Apr-13</td>
<td>Mary Luebke</td>
<td>Added reference to Accounting Services Procedure 2.2.23 Credit Card Acceptance.</td>
</tr>
<tr>
<td>Draft Version 2.0</td>
<td>26-Jul-13</td>
<td>Mary Luebke</td>
<td>Modifications made to #4.5 address comments from QSA.</td>
</tr>
<tr>
<td>Final Version 2.0</td>
<td>05-Aug-13</td>
<td>Mary Luebke</td>
<td>Added Hyperlinks &amp; Finalized</td>
</tr>
<tr>
<td>Draft Version 3.0</td>
<td>09-Sep-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Update for PCI DSS 3.0</td>
</tr>
</tbody>
</table>

## Document Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reviewed By</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 3.0</td>
<td>09-Sep-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Reviewed and finalized in 2015 with P&amp;P team.</td>
</tr>
<tr>
<td>Version 3.1</td>
<td>09/08/2016</td>
<td>Robert Wagner</td>
<td></td>
</tr>
</tbody>
</table>
1. Scope

This standard was developed to provide the primary building blocks or implementation of a uniform standard for network devices including, but not limited to, firewalls, routers, switches, VPN devices and wireless devices for all cardholder environments in the University of Wisconsin-Milwaukee (UWM) locations.

2. General Requirements in the Cardholder Data Environment

2.1 Network Device Deployment

2.1.1 The deployment of network devices in the cardholder data environment must comply with and satisfy the requirements of standards implemented by the UWM Cardholder Data Information Security Policy.

2.1.2 All network devices must be housed in a physically secure location. All network devices must be hardened as per the business requirements.

2.2 Traffic Management

2.2.1 All traffic coming from or going to addresses associated with the cardholder data environment must be managed. Only authorized traffic must be allowed to pass through the firewall and routers. All the rules pertaining to the traffic flow must be configured on a business need-to-know basis. [SAQ Req. #1.1.4(a)]

2.2.2 Where needed (e.g., to support a web-based internet facing application used to exchange confidential information), create a demilitarized zone (DMZ) to control network traffic entering and leaving the network and crossing security boundaries. [SAQ Req. #1.1.4(a)]

2.3 Network Device Configuration

2.3.1 The network device must be configured based on documented guidelines and procedures to resist penetration from internal and external attack. If the network device is hosted by a computer operating system, the underlying operating system must be configured to be secure based on the requirements of the UWM System Configuration Standards for information security.
2.3.2 For a list of trusted users, the administrator can separately allow secure shell (SSH) access to network device Command Line Interface (CLI), and Hypertext Transfer Protocol Secure (HTTPS) or Secure Sockets Layer (SSL) access to the network device browser-based interface. No unencrypted management of the device is allowed.

2.3.3 IP spoofing must be prevented by adequate controls. [SAQ #1.3.4]

2.3.4 All unnecessary ICMP traffic must be dropped.

2.3.5 Shut down all the services that are not required by the business.

2.4 Network Device Integrity

2.4.1 Network device passwords must be stored (e.g. in router configuration files) in a secured form (such as MD5 Encryption or protected file). These passwords must be changed at pre-determined frequencies as defined in the UWM Cardholder Data Information Security Policy.

2.4.2 Configure network devices properly to help resist attacks and to ensure the integrity and confidentiality of the network traffic.

2.4.3 When managing network devices, in the cardholder data environment, UWM’s active directory or LDAP authentication must not be used.

2.5 Firewall & Router Properties

2.5.1 The firewall’s and router’s rule base structure must support a “Deny all services except those specifically permitted” design policy. [SAQ Req. #1.2.1(b)]

2.5.2 Only firewalls capable of performing at least stateful inspection (dynamic packet filtering) will be permitted in the organization. Connections will be allowed in only if they are associated with a previously established session, or they are connection establishment requests. [SAQ Req. #1.3.6]
2.6 Network Device Change Control

Any change to the network device configuration or infrastructure must be documented and should be in accordance with UWM’s UITS-wide Change Management Procedure. [SAQ Req. #1.1.1]

2.7 Network Device Configuration Management

2.7.1 Backup of all the running configurations must be maintained and should be updated according to the change process.

2.7.2 Backup of updated running configurations are classified as at least sensitive and should be stored securely at offsite locations.

2.8 Authentication

2.8.1 The network devices must contain advanced authentication measures, e.g., use of biometrics devices or smart cards, or being capable of supporting dual authentication for remote access to these devices. [SAQ Req. #8.3]

2.8.2 Complex passwords must be used when accessing the firewalls and routers/switches

2.8.3 Any user who gains access to the command prompt must not have administrator privileges by default.

2.8.4 All users must be authenticated via a secure method at the network device before being granted access to that network device.

2.8.5 Terminal timeout must be configured.

2.8.6 The device must be configured according to the Password Policy found in UWM’s Cardholder Data Information Security Policy.

2.9 Network Information

2.9.1 The network devices must not permit any internal network information to be exposed through queries from external devices to, for example, Domain Name System (DNS) servers.
2.9.2 Appropriate login banners must be implemented on all network devices, where possible.

2.10 Filtering

2.10.1 Network devices must be capable of employing filtering techniques used to permit or deny services, applications, and protocols to specified network addresses as needed. The network device shall provide filtering based on relevant attributes, such as, source and destination IP address, protocol type, source and destination Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port, and inbound or outbound interface.

2.10.2 There will be no access to the cardholder data environment from the public network. In addition, there will be no outbound traffic from the cardholder data environment to the public network without being filtered through the firewall.

2.10.3 SNMP Rules
- 2.10.3.1 All network devices being monitored via SNMP must have non-default SNMP community strings.
- 2.10.3.2 Network devices not being monitored via SNMP must have SNMP disabled.
- 2.10.3.3 Rules have been established so SNMP queries are only allowed for an authorized SNMP server.

2.11 Port Restrictions

All ports should be blocked unless the merchant has documented a business requirement for the port/service to the cardholder data environment. Requests for opening ports/services will be vetted with the merchant, Network Operations and Information Security. The list of ports/services and the business rationale will be maintained by UWM. [SAQ Req. #1.1.6(a) and #1.1.6(b)]

3. Network Device Installation

3.1 Installation

The network device must be installed on a dedicated platform, either as an appliance or on a conventional computer, including optimized hardware and, where appropriate, a licensed
version of the recommended operating system. The network device must have all necessary patches installed.

3.2 Operating System Configuration

3.2.1 An operating system hosting a network device must be configured based on documented guidelines for the following:

3.2.1.1 Removal or disabling of unused network protocols, services, and applications.
3.2.1.2 Removal or disabling of unnecessary user accounts, e.g., Administrator and Guest.
3.2.1.3 Replacement of vendor passwords.
3.2.1.4 Implementation of appropriate access controls.
3.2.1.5 Configuration of audit logging controls.
3.2.1.6 Application of all relevant operating system patches and releases.

3.2.2 When configuring a network device, the administration staff must consider the configuration of other network infrastructure components such as firewalls, routers, web servers, Local Area Network (LAN) servers, etc. to ensure no adverse effect in their operation and configuration.

3.3 Authorized Administration

Only authorized administrators are allowed access to network devices to set-up, maintain, and modify security rules on UWM network devices. Access must comply with the UWM Access Control Policy.

3.4 Testing the network device

3.4.1 Verify with the merchant that all changes have been applied successfully and nothing has inadvertently been opened.

3.4.2 Scans will be performed in a timely manner to confirm no unnecessary services have been opened.
4. Logging and Alerting

4.1 Logging must be enabled. All the event logs must be monitored and trigger alerts.

4.2 The audit logs of network devices must be monitored according to the UWM Audit Log & Monitoring Policy and the Log Review Procedure.

4.3 Event log information related to the traffic passing through the network device must be exportable to reporting and analysis tools.

4.4 Event logs (audit trails) shall be available on demand online for analysis purposes for a minimum period of 90 days.

4.5 Event logs for firewalls, switches, routers, IDS, IPS and anti-virus must be archived offline for at least 365 days (one year). Event logs must be managed and maintained in a manner compliant with the UWM implemented audit and relevant standards for information security.

4.6 Connection Accounting

Detailed log information for the cardholder data environment shall be captured on every connection through the network devices. This information must include at a minimum but not limited to service type, time of connection and termination of the connection, source port, destination port, source IP address, destination IP address, packet type, and action taken.

4.7 Active Connections

The installed network devices or the related management server shall provide facilities to view in real time all connections currently active through the firewall.

4.8 Terminating a Session

The firewall or router must provide automatic facilities to terminate a single or multiple active connections upon detection of intrusion. The firewall or router must also provide manual facilities to terminate a single or multiple active connections by any authorized administrator.

4.9 Multiple Alerting Capabilities
The network device integrates with reporting and analysis tools for multiple administrator selectable alerting options including paging, audible alarms, e-mail notification and Simple Network Management Protocol (SNMP) traps for integration with third party SNMP-based network management systems.

4.10 Real-time Alerting Mechanisms

Unauthorized access attempts from the external network must be reported via a real-time alert.

5. Network Device Administration

5.1 Assigned Administrators [SAQ Req. #1.1.5]

Physical and logical access to network devices must be restricted only to assigned administrators responsible for configuration and maintenance of the devices. Logical access to a network device must be managed based on authentication. Logical access must be centrally administered.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Role/ Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Operations</td>
<td>Administration and monitoring of the firewall and other network components, such as routers/switches</td>
</tr>
<tr>
<td>Merchant</td>
<td>Application maintenance and rollout</td>
</tr>
<tr>
<td>Merchant IT Support</td>
<td>Back end operations support, query management and reporting</td>
</tr>
</tbody>
</table>

5.2 Network Access Control

The installed network device shall have the ability to define security rules using time parameters.
6. Virtual Private Networks (VPNs)

6.1 Establishing VPNs

Network devices may be employed to establish VPNs. The following requirements shall be considered when a network device hosts a VPN. Other methods of establishing VPNs can be utilized if they meet the same security requirements.

6.2 VPN Security Requirements

The primary technology requirements for VPNs shall be:

6.2.1 Strong data encryption shall protect the privacy of cardholder data for both site-to-site and client-to-site communications. [SAQ Req. #4.1(a)]

6.2.2 Two-factor authentication is required to verify remote and mobile user’s identities in the most accurate and efficient manner possible. [SAQ Req. #8.3]

6.3 VPN Connection Requirements

6.3.1 Establishment of VPNs

Any VPN technology deployed involving the UWM cardholder environment must be approved by Network Operations, Information Security and the merchant.

6.3.2 Encryption Requirement

All UWM VPNs in the cardholder environment must implement encryption methods approved by Information Security and implemented, managed, and maintained based on the UWM Key Management and Encryption Policy.

7. Network Device Authentication Communications

All authentication methods (e.g., Lightweight Directory Access Protocol (LDAP), radius, Active Directory, etc.) must communicate using encryption technologies which meet standards laid out by Key Management and Encryption Policy.
8. Time Synchronization

Network devices must be synchronized against a Central Network Time Protocol (NTP) server. All servers in the PCI environment are tied to the Active Directory or VMWare which is tied to the central NTP server (ntp.uwm.edu) for time synchronization. This is to make sure events in the logs can be correlated accurately. [SAQ Req. #10.4]

9. Review of Network Device Rule Sets

Network device rule sets and configuration standards must be reviewed at least every six months. This review will be performed by Network Administrators and the Information Security Office with validation from the merchant’s IT Support. [SAQ Req. #1.1.7(a) and #1.1.7(b)]

10. Network Device Maintenance

10.1 Education and Training

Proper and adequate training must be provided to all system and security administrators to insure appropriate maintenance and administration of the network devices.

10.2 Administrative Requirements

Administrators must maintain the configuration and rule bases continuously in accordance with the UWM business requirements and current policies. Change management must be performed in a manner compliant with the requirements of UWM’s UITS-wide Change Management Procedure.

11. Network Architecture Principles

11.1 All inbound and outbound traffic on all firewall/routers will be limited to only protocols that are necessary to the cardholder data environment. [SAQ Req. #1.2.1(a)]

11.2 Use of insecure protocols such as rlogin, telnet, and ftp are not permitted without explicit prior approval from merchant, Network Operations and Information Security.
11.3 Connections between public servers and components storing cardholder data will be restricted through firewall intermediation.

11.4 Inbound internet traffic to the internal network will be limited to IP addresses within the DMZ. [SAQ Req. #1.3.2]

11.5 As of the date of this policy, UWM does not nor shall not store any electronic cardholder data in their environment unless specifically approved by the Controller’s Office as defined in Accounting Services Procedure 2.2.23 Credit Card Acceptance. If cardholder data is approved to be stored the database hosting critical/sensitive data will be on an internal network zone, segregated from any other networks by a firewall. [SAQ Req. #1.3.7]

11.6 Network device configuration files must be secure and synchronized [for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), must have the same, secure configurations]. [SAQ Req. #1.2.2]

11.7 Perimeter firewalls will be installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data. [SAQ Req. #1.2.3]

11.8 Mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization’s network, will have personal firewall software installed and active, which must be configured by the organization to specific standards and not alterable by the employee. [SAQ Req. #1.4(a) and #1.4(b)]

11.9 Direct access between external public networks and system components storing cardholder data will not be allowed. No direct route inbound or outbound for Internet traffic from the internal network data will be permitted. [SAQ Req. #1.3.3]

11.10 Outbound traffic from cardholder applications shall only access IP addresses within the DMZ. Specific access to external IP addresses as per the client business requirements to be allowed only after prior authorization from Information Security, the merchant and Network Engineering. No unauthorized outbound traffic originating from cardholder applications will be permitted on Internet/public networks. [SAQ Req. #1.3.5]
11.11 Network Address Translation (NAT) or other technology using Request For Commands (RFC) 1918 address space must be used by firewalls/ routers to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading). Private IP addressing schema to be used in the organizational network to restrict broadcast of IP addresses from the internal network to the internet. [SAQ Req. #1.3.8]

12. Compliance

Compliance with this standard is mandatory and UWM department managers must ensure continuous compliance monitoring within their department. Compliance with the statements of this standard is a matter of periodic review by the PCI Compliance Analyst and any violation of the standard may result in corrective action as outlined in *UWM Acceptable Use of University Information Technology Resources Policy*.

The Vice Chancellor for Finance and Administrative Affairs is the owner of this document and is responsible for ensuring that this standard document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This standard was approved by the Credit Card Acceptance Committee. *This standard has been accepted by the merchant’s in each SLA. Any exception requests to this standard must be sent to the Controller’s Office for review and approval as defined in Accounting Services Procedure 2.2.23 Credit Card Acceptance.*