## Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>December 31, 2015</td>
</tr>
<tr>
<td>Added Formal Process for approving &amp; testing network connections and changes to the firewall and router configuration. Added description of groups, roles, and responsibilities for management of network components.</td>
<td>June 30, 2016</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. **FIREWALL STANDARD** ................................................................. 4  
   1.1 Scope ......................................................................................... 4  
   1.2 Purpose .................................................................................... 4  
   1.3 Roles and Responsibilities .......................................................... 4  
   1.4 Configuration .......................................................................... 5  
   1.5 Network Security Zones .............................................................. 6  
   1.6 Firewall Rulesets ...................................................................... 6  

2. **ROUTER AND SWITCH STANDARDS** ............................................. 8  
   2.1 Scope ......................................................................................... 8  
   2.2 Purpose .................................................................................... 8  
   2.3 Standard .................................................................................. 8  
   2.4 Responsibility for Standard Maintenance ..................................... 10
1. Firewall Standard

1.1 Scope
These standards cover the configuration of Missouri Botanical Garden (MBG) network firewalls and PCI network service requirements.

1.2 Purpose
To establish a set of standards for implementing and maintaining secure network firewall configurations. Including but not limited to, defining network security segments or zones within the MBG network and the type and nature of traffic which will be allowed or denied access to those zones. Also, to maintain the stability of the network and increase the security for identified resources.

1.3 Roles and Responsibilities

1.3.1. Information Technology System Administration staff
- Installation, administration, and support of firewall equipment and software
- Keeps PCI network diagrams up to date
- Keeps PCI firewall, routers and switch patches against critical security patches within one month of release, less-risky changes are installed within 2-3 months
- As approved by the Senior Manager of Telecommunications and System Administration:
  - Perform firewall configuration changes
  - Rule set configuration changes

1.3.2. Network Security Analyst
- Evaluate firewall configuration change requests and forward for approval
- Evaluate Firewall rule set change requests and forward for approval
- Documents changes and business justification in the Garden's Firewall Supporting Documentation
- Run Vulnerability equipment scans for vulnerabilities prior to ruleset change
- Run Vulnerability scans after firewall and router changes
- Quarterly review of firewall configuration, access levels and rulesets
- Regular review of firewall logs and PCI network components
- Reports to Chief Information Officer any non-compliance with the PM or Standard
- Recommends changes to the firewall PM and standard

1.3.3. Senior Manager of Telecommunications and Systems Administration
- Reviews firewall configuration recommendation and requests from Network Security Analyst
- Reviews firewall rule set recommendation and requests from Network Security Analyst

1.3.4. Chief Information Officer
- Approves the updates and changes to the Firewall PM and standard
- Addresses issues of non-compliance

1.4. Configuration

Firewalls should be configured to:
- use stateful inspection
- provide ingress filtering
- restrict inbound and outbound traffic
- not respond to external pings or traceroutes
- to Network Address Translation (NAT) internal addresses
- always change vendor-supplied defaults on firewalls, routers and switches
- including but not limited to passwords
- Simple Network Management Protocol (SNMP) community strings
- elimination of unnecessary accounts

For PCI environments:
- A firewall must exist between any wireless and PCI network blocking any non-business traffic
- must not allow outbound traffic must have business justification such as access to service provider and merchant bank
- inbound traffic must have a business justification and only allow services required
- PCI web servers must reside in the PCI DMZ
- If a credit card database is implemented it must reside in the CDE network segment
- PCI servers must use an internal RFC1918 address space

1.5 Network Security Zones

A set of clearly defined network zones, with different levels of security requirements, built to provide the proper secure levels of network access to the Garden's staff and systems.

1.5.1. Non-CDE network segment

A semi-restricted network that contains workstations and servers limited to needed services with no direct access from the Internet or to the CDE segment.

1.5.2. CDE network segment

A restricted network that contains computing devices that store, transmit or process credit card holder data. This segment has no direct access from the Internet or non-CDE segment except via business-justified access rules granted in the intersegment firewall.

1.5.3. DMZ

A sub network which contains academic and business servers which provide services over the Internet.

1.6 Firewall Rulesets

1.6.1. Inbound Connections

Inbound connections are defined as connections originating from outside the Garden network/firewall and destined for the inside of the firewall. By default the firewall will deny all inbound connections. Rules must be approved and created to allow specific inbound connections. All firewall requests must come from the system owner.

All ports opened must have accompanying justification documented within the Garden's Firewall Support Documentation.

1.6.2. Network Firewall Change Control

Network firewall configuration changes must be approved by the Senior Manager of Telecommunications and Network Administration. Any change made to any network firewall must be documented using the Garden's Network Firewall Change Control process.

For any service that needs to be open to the public, a vulnerability scan of the server is required prior to permitting Internet access.

1.6.3. Administrative Access

All administrative users must authenticate via a unique login. A backup
administrator account shall only be used when required for console access. All remote administrative access shall be encrypted via Virtual Private Network (VPN). Internal access to PCI firewalls, routers, and switches must use SSL or SSH.

1.6.4. Logging

All network firewalls will be configured to use system logging (syslog) to export its log messages to designated syslog servers. Firewalls will be configured to reject all SNMP requests. At a minimum, the firewall log will be configured to detect:

- Emergencies, such as unusable messages
- Alert, critical conditions, error and warning messages
- Logon access and configuration attempts made to the firewall
- Logs must be offloaded or copied to a secure centralized internal log server
- Logs must be retained for one year, 3 months must be immediately available

1.6.5. Logging on all network components

All network components in the PCI environment must log:

- All actions taken by any individual with root or administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms is logged
- Creation and deletion of system level objects

1.6.6. Log entries must include:

- User identification
- Type of event
- Date and time stamp
- Success or failure
- Origination of event
- Identity or name of affective component

1.6.7. Other requirements of logging

- Time-synchronization technology based on a time server which receives time signals from external sources based on International Atomic Time (TAI) or Coordinated Universal Time (UTC) (e.g., Network Time Protocol (NTP))
- Only individuals with a business need should access time data
Any changes to time settings must be logged, monitored, and reviewed
Only individuals who have a job-related need can view audit trail files
Audit trail files must be protected from unauthorized modifications
Audit trail files must be backed up promptly to a centralized log server or media that is difficult to alter
Logs must be retained for one year, 3 months must be immediately available

2. Router and Switch Standards

2.1 Scope
This standard describes a required minimal security configuration for all routers and switches connecting to a network or used in a production capacity at or on behalf of Missouri Botanical Garden.

2.2 Purpose
All routers and switches connected to Missouri Botanical Garden networks are affected. This document is broken into two sections: Baseline routers and switches, and Perimeter routers and switches. All routers and switches will be configured to the baseline standard, perimeter devices have additional required controls.

2.3 Standard

2.3.1. Baseline:
1. No local user accounts are configured on the router.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
   • IP directed broadcasts
   • TCP small services
   • UDP small services
   • All web services running on router
   • Switch interfaces set with "dynamic" port negotiation
   • Use SNMPv3 and MD5 hashing.
   • All routing updates shall be done using secure routing updates.
   • Access control lists are to be added and modified as business needs arise.
4. A primary and backup point of contact must be provided for each router and switch on the Garden’s network.

5. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. TLS is the preferred management protocol.

6. Synchronize all clocks through the use of NTP.

7. An audit and logging strategy, based on the Garden's Log Management Standard must be utilized.

8. Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.

2.3.2. Perimeter:

1. Disallow the following:
   - Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses or the Garden’s public IP space
   - Block IP packets that have the same source and destination
   - Outgoing packets at the router sourced with invalid addresses, such as RFC1918 addresses
   - All source routing
   - CDP on Internet connected interfaces
   - IP directed-broadcast

2. Implement black hole routing, or null routing

3. Disable network auto-loading via TFTP

2.3.3. Exceptions

Exceptions to this policy will be handled in accordance with the Garden’s Security Policy.

2.3.4. Review

This policy will be maintained in accordance with the Garden's Security Policy.

2.3.5. Emergencies

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the Garden's Incident Response Plan. These actions may include rendering systems inaccessible.
2.4 Responsibility for Standard Maintenance

The Chief Information Officer is responsible for ensuring that this standard is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.
3. **Process for Approval and Testing of Network Connections and Firewall and Router Configurations**

All changes to network connections, firewall or router configurations must be approved by the Senior Manager of System Administration. All changes must be tested upon completion for compliance with Firewall and Router Configuration Standards.

### 3.1 Change Requests

All changes to network connections, firewall or router configurations must be documented in a Network Change Request to the Senior Manager of System Administration. The change request must identify which devices are being changed, how and why. The Senior Manager of System Administration will review the request and approve it and enter the request into the Network Change Log.

### 3.2 Change Procedure

After the approved change has been completed, the completed action will be reported to the Senior Manager of System Administration, and the change will be recorded as completed with date in the Network Change Log.

### 3.3 Change Testing

All completed changes will be tested during the monthly TrustWave vulnerability scan to verify that network integrity has been maintained. If any new vulnerability is discovered during the scan, it will be analyzed and remedied immediately.

The completion of the vulnerability scan will be added to the Network Change Log for all changes that were included in the scan.
4. Groups, Roles and Responsibilities for Management of Network Components

4.1 Groups

The System Administration team is the only group that will manage network components.

4.2 Roles and Responsibilities

4.2.1. Senior Manager of System Administration. Leads the administration of all network and server components. Oversees daily operations of the network and servers, monitors events and warnings, reviews and approves all network changes, reviews results of vulnerability and penetration tests and remedies all vulnerabilities identified.

4.2.2. System Administrator. Monitors server and firewall components. Applies patches and system updates as required. Repairs and replaces server and firewall components when they fail. Requests changes as needed to accomplish business requirements and PCI compliance. Implements changes as approved by the Senior Manager of System Administration.

4.2.3. Network Administrator. Monitors network components. Applies patches and system updates as required. Repairs and replaces network components when they fail. Requests changes as needed to accomplish business requirements and PCI compliance. Implements changes as approved by the Senior Manager of System Administration.