CREDIT CARD SECURITY POLICIES
PCI DSS 3.2 – SYSTEM CONFIGURATION STANDARDS

Version 1.0 – October 17, 2016

CONFIDENTIAL INFORMATION
This document is the property of Missouri Botanical Garden; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Missouri Botanical Garden.
# Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>October 17, 2016</td>
</tr>
</tbody>
</table>


Table of Contents

1. INTRODUCTION AND SCOPE ................................................................. 4
   1.1 Introduction ......................................................................................... 4
   1.2 Scope of Compliance ......................................................................... 4

2. ROLES AND RESPONSIBILITIES ......................................................... 4

3. SYSTEM CONFIGURATION STANDARDS: ....................................... 4
   3.1 Unique System Identifiers ................................................................. 4
   3.2 Vendor Defaults ............................................................................... 4
   3.3 Insecure Services, Protocols, or Daemons ....................................... 4
   3.4 System Security Parameters ............................................................ 4
   3.5 One Primary Function Per Server .................................................... 4
   3.6 Only Necessary Services Enabled ..................................................... 5
   3.7 System Administrators Must Be Knowledgeable .............................. 5
1. Introduction and Scope

1.1 Introduction

This document provides the Missouri Botanical Garden's policies regarding standard configuration of systems as required by the Payment Card Industry Data Security Standard (PCI DSS) Program.

1.2 Scope of Compliance

This Policy complies with PCI DSS 3.2, Requirement 2.2.

2. Roles and Responsibilities

The Senior Manager of Systems and Network Administration is responsible for ensuring compliance with this policy by systems administration staff.

3. System Configuration Standards:

3.1 Unique System Identifiers

Every system (server, appliance, desktop computer, laptop, tablet, smartphone, network device) to be used by the Garden must be configured with a permanently assigned, unique identifier (computer name, device name, or other identification).

3.2 Vendor Defaults

- All vendor-supplied defaults will be replaced.
- Unnecessary default accounts will be eliminated.

3.3 Insecure Services, Protocols, or Daemons

- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

3.4 System Security Parameters

- Configure system security parameters to prevent misuse.
- Industry-accepted hardening standards are to be implemented and updated as new vulnerability issues are identified. (PCI Requirement 2.2)

- These standards are to be applied when new systems are configured. (PCI Requirement 2.2)

3.5 One Primary Function Per Server

- Only one primary function will be implemented for one server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)

- If virtualization techniques are used, only one primary function will be implemented per virtual system component or device. (PCI Requirement 2.2.1)
3.6 Only Necessary Services Enabled

- Only necessary services, protocols, daemons, etc., as needed for the function of the system may be enabled. All services and protocols not directly needed to perform the device’s specified function must be disabled. (PCI Requirement 2.2.2)

- All enabled insecure services, daemons, or protocols must be justified. (PCI Requirement 2.2.2)

- For any services, protocols or daemons considered insecure, additional security features must be documented and implemented. (PCI Requirement 2.2.3)

- Common security parameter settings are to be included and set appropriately on system components. (PCI Requirement 2.2.4)

- All unnecessary functionality – such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers – must be removed. (PCI Requirement 2.2.5)

- All enabled functions must be documented and support secure configuration and only documented functionality must be present on system components. (PCI Requirement 2.2.5)

3.7 System Administrators Must Be Knowledgeable

- System administrators and/or personnel that configure system components must be knowledgeable about common security parameter settings for those system components. (PCI Requirement 2.2.4)