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>June 30, 2016</td>
</tr>
</tbody>
</table>
Table of Contents

1. INTRODUCTION AND SCOPE ................................................................. 4
2. ROLES, RESPONSIBILITIES AND COMMUNICATION STRATEGIES ..... 4
3. PENETRATION TESTING METHODOLOGY ........................................... 4
1. Introduction and Scope

This document provides the Missouri Botanical Garden’s methodology for penetration testing to verify PCI compliance.

2. Roles, Responsibilities and Communication Strategies

The Senior Manager of System Administration is responsible for compliance to this methodology by Information Technology staff.

3. Penetration Testing Methodology

Missouri Botanical Garden will implement a Penetration Testing Methodology utilizing a certified outside testing service that includes the following: (PCI Requirement 11.3)

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration test to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

External penetration testing will be performed at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Internal penetration testing will be performed at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Any exploitable vulnerabilities found during penetration testing will be corrected and testing will be repeated to verify the corrections.

Missouri Botanical Garden is using network segmentation to isolate the CDE from other networks, therefore penetration tests will be performed annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.