CREDIT CARD SECURITY POLICIES
PCI DSS 3.2 – CARDHOLDER DATA TRANSMISSION POLICY

Version 1.0 – June 30, 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>June 30, 2016</td>
</tr>
</tbody>
</table>

2
Table of Contents

1. INTRODUCTION AND SCOPE ................................................................. 4
2. ROLES AND RESPONSIBILITIES............................................................. 4
3. TRANSMISSION OF CARDHOLDER DATA ........................................... 4
1. Introduction and Scope

This document provides the Missouri Botanical Garden’s methodology for transmission of cardholder data.

2. Roles and Responsibilities

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

3. Transmission of Cardholder Data

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). Only trusted keys and/or certificates can be accepted. Security protocols must be implemented to use only secure configurations, and to not support insecure versions or configurations. The proper encryption strength must be implemented for the encryption methodology in use (check vendor recommendation/best practices). For SSL/TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL. (PCI Requirement 4.1)

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user messaging technologies include email, instant messaging and chat. (PCI requirement 4.2)

This policy will be ensured to be in use and known to all affected parties. (PCI Requirement 4.3)