CREDIT CARD SECURITY POLICIES
PCI DSS 3.2 – TECHNOLOGY USAGE 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>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1. INTRODUCTION AND SCOPE ......................................................................................... 4
   1.1 Introduction ................................................................................................................. 4
2. ROLES, RESPONSIBILITIES AND COMMUNICATION STRATEGIES .......... 4
3. RISK ASSESSMENT ........................................................................................................... 4
4. CRITICAL TECHNOLOGY USE ..................................................................................... 4
1. Introduction and Scope

1.1 Introduction

This document provides the Missouri Botanical Garden's policy for governing technology use and assessing risk as required by the Payment Card Industry Data Security Standard (PCI DSS) Program.

2. Roles, Responsibilities and Communication Strategies

The Vice President, Information Technology and Chief Information Officer is responsible for compliance to this policy by all Garden staff.

3. Risk Assessment

Missouri Botanical Garden will implement a Risk Assessment process that: (PCI Requirement 12.2)

- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)
- Identifies critical assets, threats and vulnerabilities, and
- Results in a formal risk assessment.

Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005, and NIST SP 800-30.

4. Critical Technology Use

Missouri Botanical Garden has established the following usage policies for critical technologies (for example, remote-access and wireless technologies, removable electronic media, laptops, tablets, email, and Internet usage. (PCI Requirement 12.3)

4.1 Remote Access Technology Usage for PCI

Remote access technologies include the use of Citrix/Metaframe, TeamViewer, pcAnywhere, LogMeIn, or Windows Terminal.

- Explicit approval by authorized parties to use the technologies
  - All use of remote access technologies to access servers requires specific login authorization and the use of two-factor authentication.
  - Use of remote access technologies to access a desktop or laptop within the Garden's CDE requires an encrypted connection using TFS or equivalent secure protocol, such as the Garden's Fortinet VPN.
- Authentication for use of the technology
  - Authentication for remote access to servers or network equipment within the Garden's CDE require approval from the Chief Information Officer.
Authentication for remote access to desktops or laptops within the Garden's CDE require approval of the employee’s Department Head and the Senior Manager of System Administration.

- A list of all such devices and personnel with access (See also Requirements 2.4 and 11.1)
  
  See Appendix 1.

- Acceptable uses of the technologies

  Remote access by authorized personnel via two-factor authentication may be used to perform any action necessary to maintain and administer the CDE.

  The entry of credit card information via remote access to desktop or laptops within the CDE is strictly prohibited. Remote access may be utilized for information access and reporting.

- Acceptable network locations for the technologies

  Remote access may not be utilized in any public space where unauthorized personnel may observe the screen.

- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

  Remote sessions will be automatically disconnected after 15 minutes of inactivity and require a new login.

- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate de-activation after use

  Vendors and business partners may be granted remote access to the CDE with approval of the Chief Information Officer. Their activity will be monitored by IT staff and the access will be de-activated immediately after the approved activity is completed.

- Copying, moving, and storage of cardholder data via remote access onto local hard drives and removable electronic media is strictly prohibited unless explicitly authorized for a defined business need by the Chief Information Officer. Where there is an authorized business need, the data must be protected in accordance with all applicable PCI DSS Requirements.

4.2 Wireless Technology Usage for PCI

Wireless technology refers to connection to the Garden's network via WiFi. No cellular data connection is provided by the Garden into the CDE.

- Explicit approval by authorized parties to use the technologies

  Only approved devices may be used to connect to the CDE via WiFi. These devices are authorized via MAC address specifically and not via password alone.

- Authentication for use of the technology

  Only devices specifically requiring WiFi access to provide their business function, e.g. ticket scanning equipment, will be authorized to connect to the CDE via WiFi. All other WiFi devices will be blocked via internal firewall from accessing the CDE.
4.3 Removable Electronic Media for PCI

Removable electronic media includes flash drives, CDs and DVDs.

- Explicit approval by authorized parties to use the technologies
  - Copying card data or any personally identifiable data to removable electronic media is strictly prohibited.

- Authentication for use of the technology
  - No one will be authorized for use of this technology.

- A list of all such devices and personnel with access (See also Requirements 2.4 and 11.1)
  - No devices or personnel are authorized.

- Acceptable uses of the technologies
  - There is no acceptable use of this technology.

- Acceptable network locations for the technologies
  - There are no acceptable network locations for use of this technology.

4.4 Laptop/Tablet Usage for PCI

- Explicit approval by authorized parties to use the technologies
  - The policy for remote access to the CDE by laptop or tablet is covered by 4.1.
  - Storing card data on a laptop or tablet located outside the Garden's controlled CDE areas is strictly prohibited.
  - Laptops or tablets may be utilized within the Garden's controlled CDE environment like a desktop with the same PCI policies applicable. These devices are included in the routine PCI inventory.

- Authentication for use of the technology
  - Laptops and tablets may be used within the Garden's controlled CDE areas with manager authentication, like a desktop.
  - Remote access authentication is defined in 4.1.
  - Storing card data is never authorized.
o A list of all such devices and personnel with access (See also Requirements 2.4 and 11.1)
   Included in the general PCI equipment list.

o Acceptable uses of the technologies
   Laptops and tablets may only be used to access PCI data within the Garden’s controlled CDE areas.

o Acceptable network locations for the technologies
   Within a Garden-controlled CDE area

4.5 Email Usage for PCI
Transmission of any card data via email is strictly prohibited.

4.6 Internet Usage for PCI
Internet usage for PCI data includes encrypted web-browser access to card data entry screens provided by Commerce Bank and other banks.

The use of point-of-sale devices to access the Internet is strictly prohibited.

o Explicit approval by authorized parties to use the technologies
   Access to web-browser card data entry must be specifically approved by the department manager and a login/password provided by the bank.
   Internet usage from a point-of-sale device is strictly prohibited.

o Authentication for use of the technology
   A login/password must be provided by the bank for authentication to use the web-browser card data entry.
   The login/password must be revoked immediately after the authorized person no longer requires the access.

o A list of all such devices and personnel with access (See also Requirements 2.4 and 11.1)
   See Appendix 1

o Acceptable uses of the technologies
   Authorized personnel may use Internet access to enter card data.

o Acceptable network locations for the technologies
   Use of the Internet to enter card data must be confined to the Garden’s controlled CDE areas.

o Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
   The Internet connection to enter card data will automatically terminate after an inactive period as defined by the bank providing the service.
## Appendix 1 – List of Approved Technology and Personnel

<table>
<thead>
<tr>
<th>Technology</th>
<th>Device(s)</th>
<th>Personnel</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td></td>
<td>Cassandra Nelson</td>
<td>Chuck Miller</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td>Lucy Thompson</td>
<td>Chuck Miller</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td>Michael Westmoreland</td>
<td>Chuck Miller</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td>Bill Behrs</td>
<td>Chuck Miller</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td>Zubin Chandran</td>
<td>Chuck Miller</td>
</tr>
<tr>
<td>WiFi</td>
<td>Ticket Scanner 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>Ticket Scanner 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>Ticket Scanner 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>Ticket Scanner 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>