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>Revised Section 7 to apply to entire policy, not just tampering.</td>
<td>Sept 19, 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. USER AUTHENTICATION ................................................................. 4

4. REMOTE ACCESS – TWO-FACTOR AUTHENTICATION .................. 5
   4.1 Authentication Procedures ....................................................... 5
   4.2 No Use of Generic/Group IDs or Passwords ............................... 5

5. RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA .............. 6
   5.1 Facility Entry Controls ............................................................. 6
   5.2 Easily Distinguish between Onsite Personnel and Visitors ............ 6
   5.3 Control Access for Onsite Personnel to Sensitive Areas .............. 6
   5.4 Identify and Authorize Visitors .................................................. 6

6. PROTECT CARD PAYMENT CAPTURE DEVICES .......................... 7

7. VERIFY POLICY IN USE AND KNOWN .......................................... 7

8. TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA ...................................................... 8
   8.1 Audit Trails ................................................................................. 8
1. Introduction and Scope

1.1 Introduction

This document provides the Missouri Botanical Garden’s policies controlling access to computer equipment within the PCI scope 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 Requirements 8.2-8.8, 9.1-9.4, 9.9-9.10 and 10.1-10.8.

2. Roles and Responsibilities

The Chief Information Officer is responsible for ensuring compliance with this policy by all Garden staff.

3. User Authentication

At least one of the following methods is to be used to authenticate all users to access computers within the PCI scope: (PCI Requirement 8.2)

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

- All authentication credentials (such as passwords/passphrases) will be rendered unreadable during transmission and storage on all system components using strong cryptography.

- User identity must be verified before modifying any authentication credential – for example, performing password resets, provisioning new tokens, or generating new keys.

- Passwords/phrases must meet the following:
  - Require a minimum length of at least seven characters
  - Contain both numeric and alphabetic characters
  - Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

- User passwords/passphrases must be changed at least every 90 days

- Individuals will not be allowed to submit a new password that is the same as any of the last four passwords/phrases he or she has used

- Passwords/phrases will be set for first time use and upon reset to to a unique value for each user, and changed immediately after the first use.

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Using two separate passwords is not two-factor authentication. Examples of two factor authentication include remote authentication and dial-in service (RADIUS) with tokens, terminal access controller access system (TACACS) with tokens, and other technologies that facilitate two-factor authentication. (PCI Requirement 8.3)

4.1 Authentication Procedures

Authentication procedures will be documented and communicated to all users including: (PCI Requirement 8.4)

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised

4.2 No Use of Generic/Group IDs or Passwords

The use of group, shared or generic IDs, passwords, or other authentication methods is disallowed including: (PCI Requirement 8.5)

- Generic user IDs are disabled or removed
- Shared user IDs do not exist for system administration and other critical functions
- Shared and generic user IDs are not used to administer any system components

Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), the use of these mechanisms will be assigned as follows (PCI Requirement 8.6)

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access

All access to any database containing cardholder data (including access by applications, administrators, and all other users) will be restricted as follows: (PCI Requirement 8.7)

- All user access to, user queries of, and user actions on databases are through programmable methods
- Only database administrators have the ability to directly access or query databases
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)

This policy will be used and made known to all affected parties. (PCI Requirement 8.8)
5. **Restrict Physical Access to Cardholder Data**

5.1 **Facility Entry Controls**

Facility entry controls will be used to limit and monitor physical access to systems in the cardholder data environment. These controls will include: *(PCI Requirement 9.1)*

- Use video camera and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *(Sensitive areas refers to any data center, server room or any area that houses systems that store, process or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.)*

- Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. For example, areas accessible to visitors should not have network ports enables unless network access is specifically authorized.

- Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines.

5.2 **Easily Distinguish between Onsite Personnel and Visitors**

Easy distinction between onsite personnel and visitors is required to include: *(PCI Requirement 9.2)*

- Identifying new onsite personnel or visitors (for example, assigning badges)

- Changes to access requirements

- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)

5.3 **Control Access for Onsite Personnel to Sensitive Areas**

Control of physical access to the sensitive areas by onsite personnel is required as follows: *(PCI Requirement 9.3)*

- Access must be authorized and based on individual job function.

- Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. are returned or disabled.

5.4 **Identify and Authorize Visitors**

Visitors to card data environment areas must be identified and authorized as follows: *(PCI Requirement 9.4)*

- Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.

- Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.
Credit Card Data Security Policies
PCI DSS 3.1 – Computer Access Controls Policy

- Visitors are asked to surrender the badge or identification before leaving the facility, or at the date of expiration.
- A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Log must be retained for a minimum of three months, unless otherwise restricted by law.

6. Protect Card Payment Capture Devices

All devices that capture payment card data via direct physical interaction with the card must be protected from tampering and substitution. (These requirements apply to card reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.) (PCI Requirement 9.9)

An up-to-date list of devices will be maintained including the following:
- Make, model of device
- Location of device (for example, the address of the site or facility where the device is located)
- Device serial number or other method of unique identification

Device surfaces will be inspected periodically to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device.) (Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.)

Training will be provided for personnel to be aware of attempted tampering or replacement of devices. Training will include the following:
- Verify the identity of any third-party personnel claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices.)
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer.)

7. Verify Policy in Use and Known

This policy will be verified to be in use and known to all affected parties. (PCI Requirement 9.10)
8. Track and Monitor All Access to Network Resources and Cardholder Data

8.1 Audit Trails

Audit trails will be implemented to link all access to system components to each individual user. (PCI Requirement 10.1)

Automated audit trails for all system components are required to reconstruct the following events: (PCI Requirement 10.2)

- All individual user accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logic access attempts
- Use of and changes to identification and authentication mechanisms – including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges.
- Initialization, stopping or pausing of the audit logs
- Creation and deletion of system level objects

Recording of at least the following audit trail entries is required: (PCI Requirement 10.3)

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

The use of time synchronization technology is required, synchronizing all critical system clocks and times and ensuring that the following is implemented for acquiring, distributing and storing time: (PCI Requirement 10.4)

- Critical systems have the correct and consistent time
- Time data is protected
- Time settings are received from industry-accepted time sources

Audit trails must be secured so they cannot be altered, as follows: (PCI Requirement 10.5)

- Limit viewing of audit trails to those with a job-related need
- Protect audit trail files from unauthorized modifications
- Promptly back up audit trail files to a centralized log server or media that is difficult to alter
Write logs for external-facing technologies onto a log server on the internal log server or media device.

Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert.)

Logs and security events must be reviewed for all system components to identify anomalies or suspicious activity as follows:

1. All security events
2. Logs of all system components that store, process or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
3. Logs of all critical system components
4. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)

Logs of all other system components must be reviewed periodically based on the Garden's policies, as determined by the annual risk assessment.

All exceptions and anomalies identified during the review process must be followed up.

Audit trail history must be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived or restorable from backup).

This policy will be documented, verified to be in use and known to all affected parties.