## Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>June 30, 2015</td>
</tr>
<tr>
<td>Consistency edits made</td>
<td>June 30, 2016</td>
</tr>
<tr>
<td>Modified Penetration Testing section to add third party to perform and Intrusion Detection to add external IDS detection, add Solarwinds LEM to change monitoring, and multiple minor edits</td>
<td>Sept 19, 2016</td>
</tr>
<tr>
<td>Changed name of Malicious Software Policy, Section 5.</td>
<td>Oct 4, 2016</td>
</tr>
<tr>
<td>Changed name of Incident Response Plan</td>
<td>Nov 3, 2016</td>
</tr>
</tbody>
</table>
Table of Contents

Introduction and Scope .......................................................................................... 5
  Introduction ............................................................................................................ 5
  Scope of Compliance ........................................................................................... 5

Requirement 1: Build and Maintain a Secure Network ............................................. 5
  Network Documentation ....................................................................................... 5

Firewall and Router Configuration Standards ......................................................... 5

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters 6
  Vendor Defaults .................................................................................................... 6
  System Configuration Standards ......................................................................... 7
  Non-Console Administrative Access Encryption ................................................ 8
  Inventory of Systems Components ..................................................................... 8

Requirement 3: Protect Stored Cardholder Data ....................................................... 8
  Non-Console Administrative Access Encryption ................................................ 8
  Prohibited Data .................................................................................................... 8
  Displaying PAN .................................................................................................... 9
  Disk Encryption Access ........................................................................................ 9
  Cryptographic Key Protection .............................................................................. 9
  Cryptographic Key Procedures ............................................................................ 9
  Protection of Stored Cardholder Data .................................................................. 10

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks ......................................................... 10
  Transmission of Cardholder Data ....................................................................... 10

Requirement 5: Use and Regularly Update Anti-Virus Software or Programs ............... 11
  Anti-Virus ............................................................................................................. 11

Requirement 6: Develop and Maintain Secure Systems and Applications ................... 11
  Identification of Security Vulnerabilities ............................................................ 11
  Security Patches .................................................................................................. 11
  Software Development ......................................................................................... 11
  Change Control .................................................................................................... 12
  Address Common Coding Vulnerabilities ......................................................... 12

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know ............ 13
  Limit Access to Cardholder Data .......................................................................... 13

Requirement 8: Assign a Unique ID to Each Person with Computer Access ............... 14
  User Authentication ............................................................................................. 14
  Remote Access .................................................................................................... 15
  Authentication Procedures .................................................................................. 15
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

No Use of Generic/Group IDs or Passwords ................................................................. 15

Requirement 9: Restrict Physical Access to Cardholder Data ......................................... 16

Facility Entry Controls ...................................................................................................... 16

Easily Distinguish between Onsite Personnel and Visitors ........................................... 16

Control Access for Onsite Personnel to Sensitive Areas ............................................... 16

Identify and Authorize Visitors ...................................................................................... 16

Physically Secure All Media Containing Cardholder Data ............................................. 17

Destruction of Data ......................................................................................................... 17

Protect Card Payment Capture Devices ....................................................................... 17

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data ........................................................................................................... 18

Audit Trails ......................................................................................................................... 18

Requirement 11: Regularly Test Security Systems and Processes .................................... 20

Testing for Unauthorized Wireless Access Points ......................................................... 20

Vulnerability Scanning ..................................................................................................... 20

Penetration Testing .......................................................................................................... 20

Intrusion Detection ........................................................................................................... 21

Change Detection ............................................................................................................ 21

Policies and Procedures Documented, Verified and Known .......................................... 21

Requirement 12: Maintain a Policy that Addresses Information Security for All Personnel .................................................................................................................. 22

Security Policy .................................................................................................................. 22

Risk Assessment .............................................................................................................. 22

Critical Technologies Usage Policies ............................................................................. 22

Security Responsibilities .................................................................................................. 22

Information Security Management .................................................................................. 23

Security Awareness ......................................................................................................... 23

Personnel Screeing .......................................................................................................... 23

Service Providers ............................................................................................................. 23

Incident Response .......................................................................................................... 24

Reporting an Incident ..................................................................................................... 24
Introduction and Scope

Introduction

This document explains Missouri Botanical Garden's credit card security policies as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Missouri Botanical Garden management is committed to these security policies to protect information utilized by Missouri Botanical Garden in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI DSS 3.0 requirements apply to all systems that store, process, or transmit cardholder data. The Missouri Botanical Garden's cardholder environment consists of payment applications (typically point-of-sale systems) connected to the internet for card authorization, and applications that include storage and transmission of cardholder data. The application servers, disk drives, end-point workstations and point-of-sale terminals, network devices that transmit between them, and the physical spaces immediately surrounding them are within the scope of this General Policy and must be compliant with it.

Requirement 1: Build and Maintain a Secure Network

Network Documentation

A network diagram that documents all connections between the Cardholder Data Environment and other networks, including any wireless networks, and all cardholder data flows must be created and kept current. (PCI Requirement 1.1.2, 1.1.3)

The network diagram must be consistent with the Firewall and Router Configuration Standards. (PCI Requirement 1.1.4)

Firewall and Router Configuration Standards

The Firewall and Router Configuration Standards are documented in a companion Missouri Botanical Garden Policy.

A formal process must be documented for approving and testing all network connections and changes to the firewall and router configurations? (PCI Requirement 1.1.1)

A firewall is required at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. (PCI Requirement 1.1.4)

The groups, roles, and responsibilities of logical management of network components must be assigned and documented in the Firewall and Router Configuration Standards. (PCI Requirement 1.1.5)

All insecure services, protocols, and ports must be identified and security features documented in the Firewall and Router Configuration Standards and implemented for each identified service. (PCI Requirement 1.1.6)

The Firewall and Router Configuration Standards must include a documented list of services, protocols, and ports including business justification. For example HTTP, SSL, SSH and VPN protocols. (PCI Requirement 1.1.6)

The Firewall and Router Configuration Standards must require a review of firewall and router rule sets at least every six months. (PCI Requirement 1.1.7)
Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied (PCI Requirement 1.2.1)

All open ports and services must be documented. Documentation should include the port or service, source and destination, and a business justification for opening said port or service. (PCI Requirement 1.2.1)

Router configuration files must be secured from unauthorized access and synchronized – boot-up configuration must match the running configuration. (PCI Requirement 1.2.2)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports. (PCI Requirement 1.3.1)
- Limit inbound Internet traffic to IP addresses within the DMZ. (PCI Requirement 1.3.2)
- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment (PCI Requirement 1.3.3)
- Implement anti-spoofing measures to detect and block forged sourced IP addresses from entering the network. (PCI Requirement 1.3.4)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized (PCI Requirement 1.3.5)
- Firewalls must implement stateful inspection, also known as dynamic packet filtering (PCI Requirement 1.3.6)
- System components that store cardholder data must be placed in an internal network zone, segregated from the DMZ and other untrusted networks. (PCI Requirement 1.3.7)
- Implement methods to prevent the disclosure of private IP addresses and routing information to the Internet. (PCI Requirement 1.3.8)

Any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are to access the organization's network must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

The Firewall and Router Configuration Standards must be documented, in use and known to all affected parties. (PCI Requirement 1.5)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)
Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to:

- default encryption keys
- passwords
- SNMP community strings
- default passwords/passphrases on access points
- other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption for authentication and transmission of data over wireless networks. (PCI Requirement 2.1.1)

System Configuration Standards

The System Configuration Standards are documented in a companion Missouri Botanical Garden Policy.

The System Configuration Standards must include:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server
- Enabling only necessary services, protocols, daemons, etc. as required for the function of the system
- Implementing additional security features for any required services, protocols, or daemons that are considered to be insecure
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.

The System Configuration Standards must include industry-accepted hardening standards and updated as new vulnerability issues are identified. (PCI Requirement 2.2)

The System Configuration Standards must be applied when new systems are configured. (PCI Requirement 2.2)

- 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)
- 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)
- 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)
- The System Configuration Standards must include common security parameter settings. (PCI Requirement 2.2.4)
- Common security parameter settings as defined in the System Configuration Standards must be 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)
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- 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)

Non-Console Administrative Access Encryption

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must use strong cryptography for administrator access to web-based management interfaces.
- Strong cryptography must be implemented according to industry best practices and/or vendor recommendations for the technology in use.

Inventory of Systems Components

An inventory of all system components that are in scope for PCI DSS, must be maintained, including a list of hardware and software components and a description of function/use for each. (PCI Requirement 2.4)

- The inventory document must be kept current.
- Security policies and operational procedures for managing vendor defaults and other security parameters must be documented, in use and known to all affected parties. (PCI Requirement 2.5)

Requirement 3: Protect Stored Cardholder Data

Non-Console Administrative Access Encryption

All non-console administrative access will be encrypted as follows: (PCI Requirement 3.1)

- Cardholder data storage amount and retention time will be limited to that required for legal, regulatory, and business requirements.
- Defined processes must be in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons.
- Specific retention requirements will be documented for cardholder data.
- A quarterly process will be documented for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.
- All cardholder data must meet the requirements defined in the data retention policy.

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance.
This includes cardholder’s name, primary account number (PAN), expiration date, and service code. (PCI Requirement 3.2.1)

- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored after authorization under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

Missouri Botanical Garden will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI Requirement 3.3)

The PAN will be rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using one of the following approaches:

- One-way hashes based on strong cryptography (has must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of the PAN)
- Index tokens and pads (pads must be security stored)
- Strong cryptography (with associated key management processes and procedures)

Disk Encryption Access

Missouri Botanical Garden does not utilize disk encryption and PCI Requirement 3.4 is not applicable.

Cryptographic Key Protection

Missouri Botanical Garden will protect keys used to secure cardholder data against disclosure and misuse as follows: (PCI Requirement 3.5)

- Access to cryptographic keys will be restricted to the fewest number of custodians necessary.
- Secret and private cryptographic keys used to encrypt/decrypt cardholder data will be stored in one (or more) of the following forms at all times:
  - Encrypted with a key-encrypting key that is at least as strong as the data-encryption key and that is stored separately from the data-encrypting key.
  - Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device.
  - As at least two full-length key components or key shares, in accordance with industry-accepted method.
- Cryptographic keys will be stored in the fewest possible locations.

Cryptographic Key Procedures

Cryptographic Key Procedures will be documented in a companion Missouri Botanical Garden Policy Data Retention and Disposal and will include: (PCI Requirement 3.6)

- Generation of strong cryptographic keys.
- Secure cryptographic key usage.
Secure cryptographic key storage.

Cryptographic key changes for keys that reached the end of their define cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

Retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key).

Replacement of known or suspected compromised keys.

If retired or replaced cryptographic keys are retained, they will only be used for decryption verification purposes, and not used for encryption operations.

If manual clear-text key-management operations are used, the cryptographic key procedures will include split knowledge and dual control of cryptographic keys as follows:

- Procedures will require that key components are under the control of at least two people who only have knowledge of their own key components, and
- Dual control procedures will require that at least two people are required to perform any key management operations and no one person will have access to the authentication materials (for example, passwords or keys) of another.

Prevention of unauthorized substitution of cryptographic keys

Key custodians are required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

Protection of Stored Cardholder Data

Missouri Botanical Garden will document security policies and operational procedures for protecting stored cardholder data and ensure they are in use and known to all affected parties. (PCI Requirement 3.7)

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

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, SSL/TLS). 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)
The *Cardholder Data Transmission Policy* is a companion Missouri Botanical Garden Policy that defines the policies and operational procedures for encrypting transmission of cardholder data and ensures they are in use and known to all affected parties. (PCI Requirement 4.3)

**Requirement 5: Use and Regularly Update Anti-Virus Software or Programs**

**Anti-Virus**

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all known types of malicious software. (PCI Requirement 5.1, 5.1.1)

Periodic evaluations will be performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to be not commonly affected by malicious software continue to not require anti-virus software. (PCI Requirement 5.1.2)

Systems will be implemented on the network to attempt to detect zero-day malware behavior, e.g. Intrusion Detection and Prevention.

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and capable of generating audit logs. Anti-virus logs must be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2, 5.3)

The *Malicious Software Protection Policy* is a companion Missouri Botanical Garden Policy that provides policies and procedures for virus and malware protection and ensure it is in use and known to all affected parties. (PCI Requirement 5.4)

**Requirement 6: Develop and Maintain Secure Systems and Applications**

**Identification of Security Vulnerabilities**

Missouri Botanical Garden will have a process for identifying security vulnerabilities which will include the following: (PCI Requirement 6.1)

- Using reputable outside sources for vulnerability information
- Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities

**Security Patches**

All system components and software will be protected from known vulnerabilities by installing applicable vendor-supplied security patches. All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. (PCI Requirement 6.2)

**Software Development**

Missouri Botanical Garden will use software development processes based on industry standards and/or best practices to securely develop internal and external software applications (including web-based administrative access to applications) as follows: (PCI Requirement 6.3)

- All software applications will be developed in accordance with PCI DSS (for example, secure authentication and logging)
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- Information security will be included throughout the software development life cycle.
- Development, test and/or custom application accounts, user IDs, and passwords must be removed before applications become active or are released to customers.
- All custom code must be reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated procedures) to include at least the following:
  - Code changes must be reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices.
  - Code reviews ensure code is developed according to secure coding guidelines
  - Appropriate corrections are implemented prior to release
  - Code-review results are reviewed and approved by management prior to release

Change Control

Change control processes and procedures for all changes to system components must be followed and include the following: (PCI Requirement 6.4)

- Separate development/test environment from production environments and enforce the separation with access controls
- Separation of duties between development and production environment
- Production data (live PANs) are not used for testing or development
- Removal of test data and accounts before production systems become active
- Change control procedures for the implementation of security patches and software modifications must include:
  - Documentation of impact
  - Documented change approval by authorized parties
  - Functionality testing to verify that the change does not adversely impact the security of the system
  - Back-out procedures

Address Common Coding Vulnerabilities

Common coding vulnerabilities in software development processes will be addressed as follows: (PCI Requirement 6.5)

- Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.
- Develop applications based on secure coding guidelines

Common vulnerabilities to be addressed are:

- Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP, and XpPath injection flaws as well as other injection flaws.
- Buffer overflows
Insecure cryptographic storage
Insecure communications
Improper error handling
All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)

For web applications and application interfaces (internal and external), additional vulnerabilities to be addressed are:
- Cross-site scripting (XSS)
- Improper Access Control (such as insecure object references, failure to restrict URL access, and directory traversal and failure to restrict user access to functions)
- Cross-site request forgery (CRSF)
- Broken authentication and session management

For public-facing web applications, new threats and vulnerabilities will be addressed on an ongoing basis and ensure these applications are protected against known attacks by either of the following standards: (PCI Requirement 6.6)
- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods at least annually and after any changes. (Not the same as vulnerability scans performed for Requirement 11.2)
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall in front of public-facing web applications to continually check all traffic.)

Security policies and operational procedures for developing and maintaining secure systems and applications will be documented, verified to be in use and known to all affected parties. (PCI Requirement 6.7)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to Missouri Botanical Garden's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations for each role must include the following:
- Access needs for each role must be defined including system components and data resources that each role needs to access for their job function and level of privilege required (for example, user administrator, etc.) for accessing resources
- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control).
- Require documentation approval by authorized parties specifying required privileges.

An access control system for system components with multiple users will be established that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following. (PCI Requirement 7.2)
Coverage of all system components
- Assignment of privileges to individuals based on job classification and function.
- Default "deny all" setting

All security policies and operational procedures for restricting access to cardholder data will be documented, and verified to be in use and known to all affected parties. (PCI Requirement 7.3)

**Requirement 8: Assign a Unique ID to Each Person with Computer Access**

The *Firewall and Router Configuration Standards* are documented in a companion Missouri Botanical Garden Policy and defines the policies and procedures to implement proper user identification management for nonconsumer users and administrators on all system components. It includes the following: (PCI Requirement 8.1)

- Assign all users a unique ID before allowing them to access system components or cardholder data
- Control addition, deletion and modification of user IDs, credentials, and other identifier objects
- Immediately revoke access for any terminated users
- Remove/disable inactive user accounts at least every 90 days
- Manage IDs used by vendors to access, support or maintain system components via remote access as follows:
  - Enabled only during the time period needed and disabled when not in use
  - Monitored when not in use
- Limit repeated access attempts to locking out the user ID after not more than six attempts
- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

**User Authentication**

The *Computer Access Control Policy* requires at least one of the following methods to be used to authenticate all users: (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 identify 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
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- 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.

Remote Access

The *Computer Access Control Policy* requires 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)

Authentication Procedures

The *Computer Access Control Policy* requires 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

No Use of Generic/Group IDs or Passwords

The *Computer Access Control Policy* disallows the use of group, shared or generic IDs, passwords, or other authentication methods 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

The *Computer Access Control Policy* require, 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

The *Computer Access Control Policy* require 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
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- 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)

The Computer Access Control Policy for identification and authentication will be documented, verified to be in use and known to all affected parties. (PCI Requirement 8.8)

Requirement 9: Restrict Physical Access to Cardholder Data
The Computer Access Control Policy is documented in a companion Missouri Botanical Garden Policy.

Facility Entry Controls
The Computer Access Control Policy requires facility entry controls to 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.

Easily Distinguish between Onsite Personnel and Visitors
The Computer Access Control Policy requires easy distinction between onsite personnel and visitors 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)

Control Access for Onsite Personnel to Sensitive Areas
The Computer Access Control Policy requires control of physical access to the sensitive areas by onsite personnel 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.

Identify and Authorize Visitors
The Computer Access Control Policy implements procedures to identify and authorize visitors which include the following: (PCI Requirement 9.4)
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- 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.
- 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. Retain this log for a minimum of three months, unless otherwise restricted by law.

Physically Secure All Media Containing Cardholder Data

The Media Storage and Destruction Policy requires all media backups will be stored in a secure location on-site or at an off-site facility. The off-site location's security will be reviewed at least annually. (PCI Requirement 9.5)

Strict controls will be maintained over the internal and external distribution of any kind of media containing cardholder data including the following: (PCI Requirement 9.6)

- Classify media so the sensitivity of the data can be determined.
- Send the media by secured courier or other delivery method that can be accurately tracked.
- Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals.)

Strict controls will be maintained over the storage and accessibility of media containing cardholder data. Inventory logs must be maintained for all media and media inventories conducted at least annually. (PCI Requirement 9.7)

Destruction of Data

The Media Storage and Destruction Policy requires all media containing cardholder data must be destroyed when no longer needed for business or legal reasons, as follows: (PCI requirement 9.8)

- Shred, incinerate or pulp hardcopy materials so that cardholder data cannot be reconstructed
- Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

Protect Card Payment Capture Devices

The Computer Access Control Policy requires 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.)

The Computer Access Control Policy will be documented, verified to be in use and known to all affected parties. (PCI Requirement 9.10)

Relevance 10: Track and Monitor All Access to Network Resources and Cardholder Data

The Computer Access Control Policy is a companion policy to the Missouri Botanical Garden Policy.

Audit Trails

The Computer Access Control Policy requires audit trails to be implemented to link all access to system components to each individual user. (PCI Requirement 10.1)

The Computer Access Control Policy requires automated audit trails for all system components 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

The Computer Access Control Policy requires recording of at least the following audit trail entries: (PCI Requirement 10.3)

- User identification
- Type of event
The Computer Access Control Policy requires the use of time synchronization technology, 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

The Computer Access Control Policy requires audit trails to 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.)

The Computer Access Control Policy requires that logs and security events be reviewed for all system components to identify anomalies or suspicious activity as follows (Note: Log harvesting, parsing, and alerting tools can be used to meet this requirement): (PCI Requirement 10.6)

- The following items must be reviewed at least daily:
  - All security events
  - 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
  - Logs of all critical system components
  - 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.

The Computer Access Control Policy requires that audit trail history 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). (PCI Requirement 10.7)

The Computer Access Control Policy will be documented, verified to be in use and known to all affected parties. (PCI Requirement 10.8)
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, Missouri Botanical Garden will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.) (PCI Requirement 11.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.) it must be configured to generate alerts.

An inventory of authorized wireless access points must be maintained including a documented business justification. (See also PCI Requirement 2.4)

Incident response procedures must be implemented in the event unauthorized wireless access points are detected. Detection of unauthorized wireless devices must be included in the Cyber Security Incident Response Plan (see PCI Requirement 12.10).

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), Missouri Botanical Garden will perform vulnerability scanning on all in-scope systems. Scans must be performed by qualified personnel. Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. (PCI Requirement 11.2)

- Internal vulnerability scans must be repeated until passing results are obtained, or until all "high-risk" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scans must be performed by qualified personnel.

- Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures. External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

Penetration Testing

Missouri Botanical Garden will utilize a certified outside testing service to perform all penetration testing 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
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

- 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.

Intrusion Detection

Missouri Botanical Garden will use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. All traffic will be monitored at the external network firewall and at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. All intrusion-detection and prevention engines, baselines and signatures must be kept up to date. (PCI Requirement 11.4)

Change Detection

Missouri Botanical Garden has deployed Solarwinds Log and Event Manager to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and perform critical file comparisons at least weekly. (PCI Requirement 11.5)

Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modifications of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the Garden).

A process will be implemented to respond to any alerts generated by the change detection solution. See Cyber Security Incident Response Plan.

Policies and Procedures Documented, Verified and Known

This policy and operation procedures for security monitoring and testing is documented and will be verified to be in use and known to all affected parties. (PCI Requirement 11.6)
Credit Card Data Security Policies

PCI DSS 3.0 – General Policy

Requirement 12: Maintain a Policy that Addresses Information Security for All Personnel

Security Policy

Missouri Botanical Garden has established this document, Credit Card Data Security Policies, PCI DSS3.0 – General Policy which shall be published, maintained, and disseminated and that addresses how the company will protect cardholder data. This General Policy shall be reviewed at least annually and updated when the environment changes. (PCI Requirement 12.1)

Risk Assessment

Missouri Botanical Garden has established a Risk Assessment Process in the companion Technology Usage Policy 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.

Critical Technologies Usage Policies

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

This policy must include the following:

- Explicit approval by authorized parties to use the technologies
- Authentication for use of the technology
- A list of all such devices and personnel with access (See also Requirements 2.4 and 11.1)
- Acceptable uses of the technologies
- Acceptable network locations for the technologies
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate de-activation after use
- For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

Security Responsibilities

Missouri Botanical Garden’s policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)
Information Security Management

The manager of Systems and Network Administration shall be assigned as the PCI Information Security Officer and shall be responsible for information security management, as follows: (PCI Requirement 12.5)

- Establish, document, and distribute security policies and procedures
- Monitor and analyze security alerts and information, and distribute to appropriate personnel
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administer user accounts, including additions, deletions and modifications
- Monitor and control all access to data

Security Awareness

Missouri Botanical Garden will implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

- All personnel will be educated on cardholder data security on hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.
- Personnel will be required to acknowledge at least annually that they have read and understood the security policy and procedures.

Personnel Screening

Missouri Botanical Garden must screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. (PCI Requirement 12.7)

Service Providers

Missouri Botanical Garden will maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows (PCI Requirement 12.8):

- Maintain a list of service providers
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or other store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.
- Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the Garden.
Incident Response

The Cyber Security Incident Response Plan shall be a companion policy to the Missouri Botanical Garden Policy. (PCI Requirement 12.10)

The Cyber Security Incident Response Plan must address the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Analysis of legal requirements for reporting compromises
- Coverage and response of all critical system components
- Reference or inclusion of incident response procedures from the payment brands

The Cyber Security Incident Response Plan must be tested at least annually and also include:

- Designate specific personnel to be available on a 24/7 basis to respond to alerts
- Provide appropriate training of staff with security breach response responsibilities
- Include alerts from intrusion detection, intrusion prevention and file integrity monitoring systems

The Cyber Security Incident Response Plan must include a process to modify and evolve the Plan according to lessons learned and to incorporate industry developments.

Personnel must be aware of their responsibilities in detecting security incidents to facilitate the Cyber Security Incident Response Plan. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that a personnel might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud - Inaccurate information within databases, logs, files or paper records

Reporting an Incident

The PCI Information Security Officer should be notified immediately of any suspected or real security incidents involving cardholder data.

- Contact the PCI Information Security Officer to report any suspected or actual incidents. The report should be communicated to either pchelp@mobot.org or by calling 314-577-0895. On evenings and weekends always leave a voice message which will notify an on-duty person.
- No one should communicate with anyone outside of their supervisor(s) or the PCI Information Security Officer about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Communications Division.

Document any information you know while waiting for the PCI Information Security Officer to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.