<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>September 30, 2016</td>
</tr>
<tr>
<td>Minor edits made, separated System Configuration section</td>
<td>October 17, 2016</td>
</tr>
<tr>
<td>Revised Data Backup section</td>
<td>October 20, 2016</td>
</tr>
<tr>
<td>Revised Section IX</td>
<td>November 15, 2016</td>
</tr>
</tbody>
</table>
# Sensitive Data Security Policy

## Table of Contents

I. Introduction and Scope ................................................................. 5
   a) Introduction .................................................................................. 5
   b) Scope of Compliance ...................................................................... 5

II. Network Security ............................................................................. 6
   c) Firewall and Router Configuration Standards .................................. 6

III. Unique Identifiers Required .......................................................... 6
   a) Unique System Identifiers .......................................................... 6
   b) Unique User Identifiers ............................................................. 7
   c) Inventory of Systems Must be Maintained ...................................... 7

IV. Identifiers Required for Data Access ................................................. 7
   a) User Accounts .............................................................................. 7
   b) User Authentication ....................................................................... 7
   c) Remote Access ............................................................................ 8
   d) No Use of Generic/Group IDs or Passwords .................................... 8

V. Vendor-Supplied Defaults for System Passwords and Other Security Parameters ................................................. 9
   a) Vendor Defaults ........................................................................... 9

VI. System Configuration Standards .................................................... 9
    b) Non-Console Administrative Access Encryption .............................. 10

VII. Use and Regularly Update Anti-Virus Software or Programs ................................................................. 10
    a) Anti-Virus ................................................................................ 10

VIII. Maintain Secure Systems and Applications .................................. 10
    a) Identification of Security Vulnerabilities ....................................... 10
    b) Security Patches ........................................................................ 11
    c) Data Interfaces between Systems .............................................. 11

IX. Make and Maintain Backups of Sensitive Data .................................. 11
    a) Data Retention Policy ............................................................... 11
    b) Backup Frequency/Schedule .......................................................... 11
    c) Backup Retention ....................................................................... 11
    d) Backup Media Storage .............................................................. 11
       1. On-Site Backup Media Storage .................................................. 11
       2. Off-Site Backup Media Storage .................................................. 12
    e) Recovery Procedure ................................................................... 12
    f) Annual Testing of Recovery Procedure ........................................ 12

X. Restrict Access to Sensitive Data by Business Need to Know ................................. 12
    a) Limit Access to Sensitive Data .................................................... 12
b) Protect System Administration Accounts and Passwords.................................12

c) Limit Access to Master Files............................................................................13

XI. Restrict Physical Access to Sensitive Data.........................................................13
a) Facility Entry Controls ......................................................................................13

b) Easily Distinguish between Onsite Personnel and Visitors...............................14
c) Control Access for Onsite Personnel to Sensitive Areas ..................................14
d) Identify and Authorize Visitors..........................................................................14
e) Physically Secure All Media Containing Sensitive Data .....................................14
f) Destruction of Data..............................................................................................14

XII. Track and Monitor All Access to Network Resources and Sensitive Data ..........15
a) Audit Trails.........................................................................................................15

XIII. Regularly Test Security Systems and Processes ...............................................15
a) Testing for Unauthorized Wireless Access Points ..............................................15
b) Vulnerability Scanning .......................................................................................15
c) Penetration Testing .............................................................................................15
d) Intrusion Detection ..............................................................................................16
e) Change Detection ...............................................................................................16

XIV. Maintain a Policy that Addresses Information Security for All Personnel ........16
a) Security Policy ....................................................................................................16
b) Critical Technologies Usage Policies .................................................................16
c) Security Responsibilities ......................................................................................17
d) Information Security Management ......................................................................17
e) Security Awareness .............................................................................................17
f) Personnel Screening ...........................................................................................17
g) Service Providers ...............................................................................................18

XV. Incident Response .............................................................................................18
I. Introduction and Scope
   
a) Introduction

This document provides Missouri Botanical Garden's security policies for sensitive data. Missouri Botanical Garden management is committed to these security policies to protect sensitive information utilized by Missouri Botanical Garden in attaining its business goals. All employees are required to adhere to the policies described within this document.

b) Scope of Compliance

Sensitive information is defined as any of the following:

- Non-public financial data – e.g., pay records with employee names, private donations or grants
- Cardholder data as defined by the Payment Card Industry Data Security Standard
- Employee personal information – e.g., social security number, compensation, performance history, non-public private data
- Member or donor personal information – non-public personal data like address, phone number, relations, and donation or spending data

This policy applies to all systems and software applications that store, process, or transmit sensitive data. Security of credit cardholder data is governed by separate PCI Credit Card Data Security Policies.

The Missouri Botanical Garden's non-cardholder sensitive software applications consist of:

On-Premise Sensitive Software Applications
- Serenic/Navision accounting system and related applications

Cloud-Based Sensitive Software Applications
- Ceridian DayForce payroll and human resources system
- Cervis volunteer management system
- ApplicantPro recruiting system

The following credit cardholder software applications are governed by the PCI Credit Card Data Security Policies:

On-Premise PCI Cardholder Software Applications
- Blackbaud Raiser's Edge
- Ungerboeck EBMS/iEBMS
- Gateway Ticketing Galaxy
- Liberty4 Consignment

Cloud-Based PCI Cardholder Software Applications
- eGalaxy ticketing webstore
- Blackbaud NetCommunity
- Volusion publication webstore
The application servers, disk drives, off-site data storage, end-user workstations, network devices and transmit sensitive data between them that are not included in the PCI Cardholder Data Environment are within the scope of this Sensitive Data Security Policy and must be compliant with it.

II. Network Security

c) Firewall and Router Configuration Standards

1. The Firewall and Router Configuration Standards are documented in the Missouri Botanical Garden PCI Security Policy. The security provided by these standards is also applicable to securing sensitive data.

2. A formal process must be documented for approving and testing all network connections and changes to the firewall and router configurations.

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

4. 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.

5. Router configuration files must be secured from unauthorized access and synchronized – boot-up configuration must match the running configuration.

6. Firewall configuration must prohibit direct public access between the Internet and any sensitive data system component as follows:
   - Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports.
   - Limit inbound Internet traffic to IP addresses within the DMZ.
   - Implement anti-spoofing measures to detect and block forged sourced IP addresses from entering the network.
   - Firewalls must implement stateful inspection, also known as dynamic packet filtering.
   - Implement methods to prevent the disclosure of private IP addresses and routing information to the Internet.

7. 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.

III. Unique Identifiers Required

a) Unique System Identifiers

Every system (server, appliance, desktop computer, laptop, tablet, smartphone, network device) to be used by the Garden must be configured with a permanently assigned, unique identifier (computer name, device name, or other identification)
b) Unique User Identifiers

Every user of the Garden's network must have an assigned unique identifier (user name) before being allowed to log on to the Garden's network, sensitive system components or data. Microsoft Active Directory will be used to assign, maintain and control unique user identifiers and passwords and enforce network access security. Only authorized Active Directory usernames will be allowed to log on to the Garden's network.

Access to the Garden's business systems/ software applications requires first access to the Active Directory system and then either the Active Directory credentials are provided to the software application or a second unique username and password is required. Administration and control of the software application usernames and passwords are administered by Application Security Administrators. The Application Security Administration Policy provides the procedures and responsibilities for software application security.

c) Inventory of Systems Must be Maintained

An inventory of all system devices with their unique identifiers will be maintained by the automated Altiris Inventory Management system and the Computers Database system. The Manager, User Support is responsible to administer, update and maintain these inventory systems.

IV. Identifiers Required for Data Access

a) User Accounts

The Application Security Administrators will:

- Control addition, deletion and modification of user IDs, credentials, and other identifier objects
- Immediately revoke access and cancel passwords for any terminated users
- Remove/disable inactive user accounts at least every 90 days
- Manage IDs used by vendors to access, support or maintain sensitive 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 five (5) 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 workstation or session.

b) User Authentication

1. At least one of the following methods is to be used to authenticate all users to logon to the Garden's network or access sensitive systems:

   - 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

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

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

4. 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.

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

6. 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.

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

c) Remote Access

1. Two-factor authentication must be used for remote access (network-level access originating from outside the network) to sensitive systems by employees, administrators, and third parties.
   • Missouri Botanical Garden will use the Duo two-factor authentication system for all remote access to sensitive systems.

d) No Use of Generic/Group IDs or Passwords

1. The use of group, shared or generic IDs, passwords, or other authentication methods to access sensitive systems is disallowed including:
   o Generic user IDs are disabled or removed
   o Shared user IDs do not exist for system administration and other critical functions
   o Shared and generic user IDs are not used to administer any system components

2. All access to any database containing sensitive data (including access by applications, administrators, and all other users) will be restricted as follows:
   o All user access to, user queries of, and user actions on databases are through programmable methods
   o Only database administrators have the ability to directly access or query databases
   o Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)
V. Vendor-Supplied Defaults for System Passwords and Other Security Parameters

a) Vendor Defaults

1. 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.

2. 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

3. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission of data over wireless networks.

VI. System Configuration Standards

1. The System Configuration Standards are documented in a companion Missouri Botanical Garden Policy and also apply to Sensitive Data Systems.

2. The System Configuration Standards 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.

3. The System Configuration Standards include industry-accepted hardening standards and are updated as new vulnerability issues are identified.

4. The System Configuration Standards must be applied when new systems are configured.
   - 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.
   - If virtualization techniques are used, only one primary function will be implemented per virtual system component or device.
   - 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.
   - All enabled insecure services, daemons, or protocols must be justified.
For any services, protocols or daemons considered insecure, additional security features must be documented and implemented.

System administrators and/or personnel that configure system components must be knowledgeable about common security parameter settings for those system components.

The System Configuration Standards include common security parameter settings.

Common security parameter settings as defined in the System Configuration Standards must be set appropriately on system components.

All unnecessary functionality – such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers – must be removed.

All enabled functions must be documented and support secure configuration and only documented functionality must be present on system components.

b) Non-Console Administrative Access Encryption

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

VII. Use and Regularly Update Anti-Virus Software or Programs

a) 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.

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 as such.

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.

The Anti-virus and Malware Protection Policy is a companion Missouri Botanical Garden Policy that provides policies and procedures for malware protection.

VIII. Maintain Secure Systems and Applications

a) Identification of Security Vulnerabilities

1. Missouri Botanical Garden will have a process for identifying security vulnerabilities which will include the following:
   - Using reputable outside sources for vulnerability information
Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities

b) Security Patches
1. 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 within one month of release. This includes relevant patches for operating systems and all installed applications.

c) Data Interfaces between Systems
1. Where critical business systems need to interface to exchange sensitive data, the interchange must be configured to be secure using TLS encryption protocol or similar secure method.
2. Interfaces between business systems must include appropriate controls to ensure the complete and accurate transfer of data. These controls may be governed by the sending or receiving system or both using hashtags, CRC checks, record counts or other method of verifying completeness.

IX. Make and Maintain Backups of Sensitive Data

a) Data Retention Policy
The Garden's Document Retention Policy governs the retention of all documents and data. The Electronic Document Retention Policy - IT Addendum extends the overall document retention policy to electronic documents.

b) Backup Frequency/Schedule
All sensitive data will be backed up for protection and business continuity contingency.

Backups will be performed according to the following schedule.

VM servers: Full backup weekly starting on Sunday. Differential backups Monday thru Friday.


Application servers-Non SQL: Full backup starting on Saturday. Differential backups Monday thru Friday. Baremetal backup monthly starting on Saturday.


c) Backup Retention
The Garden's backup retention policy is to retain data for a minimum of three months through the use of online storage and removable storage.

d) Backup Media Storage
The Missouri Botanical Garden utilizes Unitrends 833 backup devices with a 12TB removable drive archive. The archive consists of 4 3TB removable drives. Each 833 device has three sets of removable archives.

1. On-Site Backup Media Storage
The Missouri Botanical Garden utilizes 4 Unitrends 833 backup devices. These devices have a 20 TB online storage array each. In addition there is a 12 TB removable drive archive attached to each device. This 12 TB archive consists of four 3TB drives. The mounted media is the current archive. An additional set is stored in the locked server room where there 833 devices reside.
Sensitive Data Security Policy

2. Off-Site Backup Media Storage
One archive set per Unitrends 833 device is stored off site every month at an Iron Mountain storage facility.

e) Recovery Procedure
The Garden’s Recovery Procedure details the recovery of all files and systems.

f) Annual Testing of Recovery Procedure
The Annual Testing of the Recovery Procedure is documented in the previously mentioned Garden’s Recovery Procedure.

X. Restrict Access to Sensitive Data by Business Need to Know

a) Limit Access to Sensitive Data
1. Access to Missouri Botanical Garden's sensitive system components and data is limited to only those individuals whose jobs require such access.

2. Role-based access controls for sensitive software applications are governed by Application Security Administrators. The policies and procedures governing Application Security Administrators are provided in the Application Security Administration Policy. Application Security Administrators must regularly review the role-based access controls to ensure that permissions are appropriate to the business need and controls are removed for employees whose role has changed or has been transferred or terminated.

3. Role-based access controls for servers, network components, and other system devices are governed by the Senior Manager of Systems and Network Administration. The Senior Manager of Systems and Network Administration must regularly review the role-based access controls to ensure that permissions are appropriate to the business need and controls are removed for employees whose role has changed or has been transferred or terminated.

4. Access limitations for each access 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 of approval by authorized parties specifying required privileges. Email records of approval will be acceptable documentation.

5. All security policies and operational procedures for restricting access to sensitive data will be documented, and verified to be in use and known to all affected parties.

b) Protect System Administration Accounts and Passwords
1. System Administrator accounts must be kept confidential and not shared outside the System Administration staff.
2. System Administrator passwords must be kept in an encrypted storage location available to designated System Administration staff, so the passwords may be obtained in emergency or unusual situations, such as incapacitation of system administrator.

3. Strong encryption must be used to secure the System Administration passwords storage.

c) Limit Access to Master Files

1. Master files are defined as a collection of records pertaining to one of the main subjects of an information system, such as customers, employees, products and vendors. Master files contain descriptive data, such as name and address, as well as summary information, such as amount due and year-to-date sales. Master files in the Garden’s critical business systems are primarily tables within a database. These include:

   On-Premise Master Files
   • Serenic/Navision – Vendors, Payees, Projects
   • Blackbaud Raiser’s Edge – Constituents, Members, Donors
   • Ungerboeck EBMS – Customers
   • Liberty4 Consignment – Customers, Products
   • Galaxy – Customers, Tickets

   Cloud-based Master Files
   • Ceridian DayForce – Employees
   • Cervis – Volunteers
   • ApplicantPro – Job applicants

2. Changes to master files/tables may only be made by users who have been given system administration authority by an Application Security Administrator. The policies and procedures governing Application Security Administrators are provided in the Application Security Administration Policy.

3. Changes to master tables are tracked by the applicable software application. Changes must monitored by application security administrators.

XI. Restrict Physical Access to Sensitive Data

a) Facility Entry Controls

1. Facility entry controls will be used to limit and monitor physical access to sensitive data systems. These controls will include:

   • 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 sensitive data.)

   • Implement physical and/or logical controls to restrict access to publicly accessible network jacks. Visitors will be escorted at all times in areas with active network jacks. Network jacks located in public areas and areas accessible to visitors will be disabled and only enabled when network access is explicitly authorized.
Sensitive Data Security Policy

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

b) Easily Distinguish between Onsite Personnel and Visitors
   1. Easy distinction between onsite personnel and visitors in sensitive data areas is required to include:
      - Identifying new onsite personnel or visitors (for example, assigning badges)
      - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)

c) Control Access for Onsite Personnel to Sensitive Areas
   1. Physical access to the sensitive areas by onsite personnel must be controlled as follows:
      - 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.

d) Identify and Authorize Visitors
   1. Procedures will be implemented to identify and authorize visitors which include the following:
      - Visitors are authorized before entering, and escorted at all times within sensitive data areas.
      - 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 sensitive 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.

e) Physically Secure All Media Containing Sensitive Data
   1. All media backups containing sensitive data will be stored in a secure location on-site or at an off-site facility. The off-site locations security will be reviewed at least annually.
      1. Strict controls will be maintained over the internal and external distribution of any kind of media containing sensitive data including the following:
         - 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.)
      2. Strict controls will be maintained over the storage and accessibility of media containing sensitive data. Inventory logs must be maintained for all media and media inventories conducted at least annually.

f) Destruction of Data

All media containing sensitive data must be destroyed when no longer needed for business or legal reasons, as follows:
Sensitive Data Security Policy

- Shred, incinerate or pulp hardcopy materials so that financial data cannot be reconstructed

XII. Track and Monitor All Access to Network Resources and Sensitive Data

a) Audit Trails
1. Audit trails must be implemented to link all access to system components to each individual user.
2. 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).

XIII. Regularly Test Security Systems and Processes

a) Testing for Unauthorized Wireless Access Points
1. At least quarterly, Missouri Botanical Garden will perform testing to ensure there are no unauthorized wireless access points present in the sensitive system 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.)
2. If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.) it must be configured to generate alerts
3. An inventory of authorized wireless access points must be maintained including a documented business justification.
4. Incident response procedures must be implemented in the event unauthorized wireless access points are detected.

b) Vulnerability Scanning
1. 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 sensitive systems. Scans must be performed by qualified personnel.
   - Internal vulnerability scans must be repeated until passing results are obtained, or until all "high-risk" vulnerabilities are resolved. Scans must be performed by qualified personnel.
   - Quarterly external vulnerability scan results must have no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures. Perform rescans as needed, until passing scans are achieved.

c) Penetration Testing
1. Missouri Botanical Garden will utilize a certified outside testing service to perform all penetration testing that includes the following:
   - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
   - Includes coverage for critical systems
   - Includes testing from both inside and outside the network
Sensitive Data Security Policy

- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests
- 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.

2. 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).

3. 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).

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

d) Intrusion Detection

1. 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 critical points in the sensitive data environment, and alert personnel to suspected compromises. All intrusion-detection and prevention engines, baselines and signatures must be kept up to date.
   - The Fortinet FortiGate Intrusion Prevention module will be used to perform intrusion detection and prevention at the Internet perimeter and at critical points within the sensitive data environment.

e) Change Detection

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

2. A process will be implemented to respond to any alerts generated by the change detection solution.

XIV. Maintain a Policy that Addresses Information Security for All Personnel

a) Security Policy

Missouri Botanical Garden has established this document, Sensitive Data Security Policy, which shall be published, maintained, and disseminated and that addresses how the company will protect sensitive data. This policy shall be reviewed at least annually and updated when the environment changes.

b) 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.
This policy includes 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
- 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 sensitive data via remote-access technologies, prohibit the copying, moving, and storage of sensitive data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

c) Security Responsibilities

Missouri Botanical Garden's policies and procedures must clearly define information security responsibilities for all personnel.

d) Information Security Management

The Senior Manager of Systems and Network Administration shall be responsible for information security management, as follows:

- 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

e) Security Awareness

Missouri Botanical Garden will make all personnel aware of the importance of sensitive data security.

- All personnel will be educated on sensitive data security on hire and at least annually.
- Personnel will be required to acknowledge at least annually that they have read and understood the security policy and procedures.

f) 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.
g) Service Providers

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

- Maintain a list of service providers
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of sensitive data the service providers possess or otherwise store, process or transmit on behalf of the Garden, or to the extent that they could impact the security of the Garden's sensitive data environment.
- Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

XV. Incident Response

For response to cyber security incidents, including credit card data incidents, refer to the companion Cyber Security Incident Response Plan.