CYBER SECURITY INCIDENT RESPONSE PLAN

INCLUDING
PCI DSS 3.2

Version 2.0 – November 2, 2016

CONFIDENTIAL INFORMATION

This document is the property of Missouri Botanical Garden; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Missouri Botanical Garden.
## Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>October 17, 2016</td>
</tr>
<tr>
<td>Merged PCI Incident Response</td>
<td>November 2, 2016</td>
</tr>
</tbody>
</table>
CYBER SECURITY INCIDENT RESPONSE CHECKLIST

1. If cyber incident (including a credit card data incident) is detected or suspected, notify a member of the Cyber Security Incident Response Team immediately then contact all members of the Team and arrange a meeting/conference call to assess the incident.

2. The Cyber Security Incident Response Team will determine the nature and severity of the incident. If the incident is not a data breach, e.g. paper left on a desk, determine the extent of the exposure and the appropriate response. If the incident is suspected to be a data breach, continue this checklist.

3. The Cyber Security Officer will call the AIG Cyber Breach Team (877-890-1259) immediately and engage them to start the assessment to confirm that a data breach has occurred. They will recommend specialists and best steps to follow.

4. The Cyber Security Incident Response Team will develop a communications plan immediately. All communications will be handled by the Communications Division. Card providers must be notified immediately after a data breach has been confirmed.

5. Computer Systems Procedures

   • Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
   • Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   • Ensure compromised system(s) is/are isolated on/from the network.
   • Gather, review and analyze the logs and related information from various central and local safeguards and security controls.
   • Preserve logs and electronic evidence.
   • Log all actions taken.
   • If a wireless network is involved, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
   • Be on "high" alert and monitor all systems with cardholder data.
   • Conduct appropriate forensic analysis of compromised system.
   • Contact internal and external departments and entities regarding system outages and expected plans as appropriate and consistent with the communications plan.
   • Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
   • Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

6. The Cyber Incident Response Team will work together with the AIG Cyber Breach Team to carry out this Incident Response Plan to properly respond to the data breach, including notification of the card providers if a credit card data incident is involved.
Contents

1. INTRODUCTION AND SCOPE ................................................................. 5
   1.1 Introduction ........................................................................................ 5
   1.2 Scope of Compliance ........................................................................... 5

2. ROLES, RESPONSIBILITIES AND COMMUNICATION STRATEGIES ..... 6
   2.1 Roles ....................................................................................................... 6
   2.2 Responsibilities ................................................................................... 6
   2.3 Communication Strategy ..................................................................... 7

3. CYBER INCIDENT RESPONSE PROCEDURES .................................... 7
   3.1 Definitions .......................................................................................... 7
   3.2 Reporting an Incident ....................................................................... 8
   3.3 Response to an Incident .................................................................... 8
   3.4 Notifying Credit Card Companies ......................................................... 8
   3.5 Eradication and Recovery ................................................................. 8

4. BUSINESS RECOVERY AND CONTINUITY PROCEDURES ............ 8

5. DATA BACKUP PROCESSES ............................................................. 9

6. ANALYSIS OF LEGAL REQUIREMENTS FOR REPORTING COMPROMISES ................................................................. 9

7. COVERAGE AND RESPONSES OF ALL CRITICAL SYSTEM COMPONENTS ................................................................. 9

8. REFERENCE OR INCLUSION OF INCIDENT RESPONSE PROCEDURES FROM THE PAYMENT BRANDS ................................................................. 9

9. ANNUAL TESTING OF THE PLAN ....................................................... 9

10. 24X7 RESPONSE ................................................................................. 9

11. TRAINING ............................................................................................... 10

12. SYSTEM ALERTS .................................................................................... 10

13. MODIFICATION OF THE PLAN ........................................................... 10

APPENDIX A - AIG CYBEREDGE BREACH RESOLUTION TEAM .......... 11

APPENDIX B – CREDIT CARD COMPANY NOTIFICATION .................. 12

   MasterCard Specific Steps: ...................................................................... 12
   VISA U.S.A. Specific Steps: ..................................................................... 13
   Discover/Experian Specific Steps: ........................................................... 15
   American Express Specific Steps: .......................................................... 16
1. Introduction and Scope

1.1 Introduction

This document provides the Missouri Botanical Garden's Incident Response Plan for a cyber or information system incident. This Incident Response Plan is required by the Payment Card Industry Data Security Standard (PCI DSS) Program for any incident involving credit card data. Missouri Botanical Garden management is committed to this plan and policies to respond to incidents involving information systems utilized by Missouri Botanical Garden in attaining its business goals. All employees are required to adhere to the policies described within this document.

1.2 Scope of Compliance

This Plan applies to any incident involving information systems, networks, or data, including credit card data. Incidents potentially involving credit card data require contacting credit card providers and addressing specific issues related to credit card data.

This Plan complies with Payment Card Industry Data Security Standard (PCI DSS) 3.2 Requirement 12.10.

PCI DSS 3.2 Requirement 12.10 requires the following:

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses 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 backup 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

12.10.2 Review and test the plan at least annually.

12.10.3 Designate specific personnel to be available on a 24x7 basis to respond to alerts.

12.10.4 Provide appropriate training to staff with security breach response responsibilities

12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
2. Roles, Responsibilities and Communication Strategies

A Cyber Security Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of confidential information, and other events with serious information security implications. The Cyber Security Incident Response Team’s mission is to prevent a serious loss of revenue, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Cyber Security Incident Response Team is responsible for putting the plan into action.

2.1 Roles

The Cyber Security Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Cyber Security Officer will coordinate these investigations.

### Missouri Botanical Garden Cyber Security Incident Response Team

<table>
<thead>
<tr>
<th>Position</th>
<th>Person</th>
<th>Phone</th>
<th>EMail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security Officer, VP-IT &amp; CIO</td>
<td>Chuck Miller</td>
<td>314-577-9419</td>
<td><a href="mailto:chuck.miller@mobot.org">chuck.miller@mobot.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>314-614-6952 (cell)</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>Peggy Lents</td>
<td>314 577-0245</td>
<td><a href="mailto:peggy.lents@mobot.org">peggy.lents@mobot.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>314 973-3186 (cell)</td>
<td></td>
</tr>
<tr>
<td>Chief Operating Officer</td>
<td>Bob Woodruff</td>
<td>314 577-5142</td>
<td><a href="mailto:bob.woodruff@mobot.org">bob.woodruff@mobot.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(cell)</td>
<td></td>
</tr>
<tr>
<td>Legal Counsel</td>
<td>Frank Wolff, Bryan Cave</td>
<td>314-259-2330</td>
<td><a href="mailto:fwolff@bryancave.com">fwolff@bryancave.com</a></td>
</tr>
<tr>
<td>AIG Cyber Breach Team</td>
<td>To be assigned by AIG</td>
<td>877-890-1259</td>
<td><a href="mailto:CyberEdge@aig.com">CyberEdge@aig.com</a></td>
</tr>
<tr>
<td>Controller</td>
<td>Cheryl Mill</td>
<td>314 577-5115</td>
<td><a href="mailto:cheryl.mill@mobot.org">cheryl.mill@mobot.org</a></td>
</tr>
<tr>
<td>VP Human Resources</td>
<td>Rebecca Ingram</td>
<td>314-577-5122</td>
<td><a href="mailto:rebecca.ingram@mobot.org">rebecca.ingram@mobot.org</a></td>
</tr>
<tr>
<td>Sr. VP Institutional Advancement</td>
<td>Donna McGinnis</td>
<td>314-577-9495</td>
<td><a href="mailto:donna.mcginnis@mobot.org">donna.mcginnis@mobot.org</a></td>
</tr>
<tr>
<td>Sr. Manager, System &amp; Network Administration</td>
<td>Cassandra Nelson</td>
<td>314-577-0813</td>
<td><a href="mailto:cassandra.nelson@mobot.org">cassandra.nelson@mobot.org</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>314-303-4731</td>
<td></td>
</tr>
</tbody>
</table>

2.2 Responsibilities

**Cyber Security Officer** – Responsible for overall coordination of the response to an incident.
Communications – Responsible for all communications inside and outside the Garden regarding an incident.

Chief Operating Officer – Responsible to investigate the financial and operational impacts of an incident and interact with financial entities such as banks.

Legal Counsel – Responsible to assess the legal aspects of an incident and provide legal counsel to the Garden after an incident.

AIG Cyber Breach Team – Responsible to assist the Garden with assessment of the incident, response and containment, mitigation and resolution, engagement of forensic analysts and communications. (See Appendix A).

Controller – Responsible to assist the CFO with financial impact assessments, financial information requests, reports and other information needed to respond to the incident.

VP Human Resources - Responsible to assist the CSO with sensitive data involving employees, volunteers or related personnel as needed to respond to the incident.

Sr. VP, Institutional Advancement - Responsible to assist the CSO with sensitive data involving constituents, donors, members, or related individuals as needed to respond to the incident.

Sr. Manager, Systems & Network Administration – Responsible to investigate system and data incidents, contain any system or data breach, protect systems and data for forensic analysis, mitigate any breach, enable backup systems, provide reports and information to respond to the incident.

2.3 Communication Strategy

The Communications Division will be the single source of all communications outside the Garden after any incident in consultation with the Cyber Security Incident Response Team. The AIG CyberEdge Breach Resolution Team will also provide advice and assistance to the Communications Division. The Garden will communicate with all parties as required by law, regulation and PCI requirements.

PCI-Specific: The Garden will communicate with the payment card providers in accordance with their prescribed procedures (see Appendix B).

3. Cyber Incident Response Procedures

3.1 Definitions

An incident is defined as a suspected or confirmed ‘data compromise’. A ‘data compromise’ is any situation where there has or may have been unauthorized access to a system, network or hard copy files where Garden sensitive data or credit cardholder data is collected, processed, stored or transmitted. Garden sensitive data is defined in the Garden's Sensitive Data Security Policy. A ‘data compromise’ can also involve the suspected or confirmed loss or theft of any material or records that contain sensitive or cardholder data.

A breach occurs when a confirmed, unauthorized acquisition, modification or destruction of Garden sensitive or credit cardholder data has taken place.
3.2 Reporting an Incident

A department that reasonably believes it may have an incident or breach of sensitive information, or of systems related to the PCI environment in general, must inform any member of the Cyber Incident Response Team. After being notified of a compromise, the Cyber Incident Response Team, along with other designated Garden staff, will implement the Cyber Incident Response Plan.

- Contact User Support to report any suspected or actual incidents. The report should be communicated 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 Cyber Security Incident Response Team 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 Cyber Security Incident Team 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.

**PCI-Specific:** Discovery of an unauthorized wireless access point attached to the Garden’s network will constitute an incident that must be reported to the PCI Security Incident Team and the wireless access point disconnected immediately from the network. The incident must be investigated to determine if a breach has occurred.

3.3 Response to an Incident

(See Page 3, Cyber Security Incident Response Checklist)

In response to a reported systems incident, the Cyber Incident Response Team and designees will follow the procedures listed in the Cyber Security Incident Response Checklist.

3.4 Notifying Credit Card Companies

**PCI-Specific:** The credit card companies have individually specific requirements that the Incident Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix B for these requirements.

3.5 Eradication and Recovery

Once the breach has been contained, eradication and recovery should be carefully executed. The Garden must be diligent to eradicate all pieces of malware deployed by the attacker. Failing to do so may allow the attacker to recover remote access by using backdoors or Trojan applications installed during the initial intrusion.


In the event that any critical business system is taken offline for a significant amount of time, the Garden's Business Continuity Plan will be activated. A new server might be required that would be restored from system backups.
5. Data Backup Processes

All business systems are routinely backed up to secondary data storage using the UniTrends backup system. In the event of a cyber or cardholder data breach, the affected systems will be immediately disconnected from the network but not turned off. Full system image backups will be made of each system without compromising the integrity of the data. Forensic investigators will then be engaged to perform the needed investigations and evidence gathering.

6. Analysis of Legal Requirements for Reporting Compromises

Missouri Botanical Garden has acquired a Cyber Liability insurance policy from AIG which includes a CyberEdge Breach Resolution Team (Appendix A) to provide legal consulting and representation in the event of a sensitive or credit cardholder data security incident. AIG’s CyberEdge Breach Resolution Team maintains up-to-date knowledge of cyber incident requirements, current regulations and law applicable to cyber incidents. AIG will advise and coordinate with the Cyber Incident Response Team and the Garden’s legal counsel on the required reporting in the event of an incident as part of the incident response procedures.

7. Coverage and Responses of All Critical System Components

The Solarwinds Log and Event Management System will continuously monitor all critical business and Card Data Environment equipment logs and may generate alerts in the event of suspicious activity. These alerts may be sufficient to initiate a security incident and follow the response procedures defined in this Plan.

8. Reference or Inclusion of Incident Response Procedures From The Payment Brands

**PCI-Specific:** The credit card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix B for these requirements.


This Incident Response Plan will be reviewed and tested annually.

10. 24x7 Response

The primary method for reporting an incident shall be via the IT department's User Support line which is manned continuously during business hours and from Friday evening through Monday morning via an automated process that alerts an assigned person.

The secondary method for reporting an incident during non-business, weekday hours will be to contact the VP-IT & CIO via cell phone 24x7 and secondarily the Senior Manager,
Systems and Network Administration, also by cell phone. Contact numbers are provided in Section 2.1.

11. Training
All members of the Cyber Incident Response Team will be trained in the following areas at minimum:

- Initial incident response procedures
- Importance of incident reporting.
- Electronic evidence preservation
- Incident response best practices
- Legal implications of an incident
- **PCI-Specific:** Requirements of the card providers

Refresher training will be conducted annually at the time of annual Plan review and testing.

All Garden staff who work with sensitive or in the Card Data Environment will be trained in incident awareness and how to identify an incident or breach.

The AIG CyberEdge Risk Tool may be utilized to assign training and track compliance.

Training may be conducted online, via videos, or via instructors.

12. System Alerts
The Solarwinds Log and Event Management System will be used to consolidate all system alerts from intrusion detection, intrusion prevention, firewalls and file integrity monitoring systems and generate alerts to System Administration.

13. Modification of the Plan
This Incident Response Plan will be reviewed during the annual testing and updated with current information and adjustments to procedures will be made as needed.
APPENDIX A - AIG CYBEREDGE BREACH RESOLUTION TEAM

http://www.aig.com/_1247_412514.html#
MasterCard Specific Steps:

Refer to documentation online at:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. **Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).**
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.
VISA U.S.A. Specific Steps:

Refer to documentation online at http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

In the event of a security breach, the Visa U.S.A. Operating Regulations require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the VISA U.S.A. Cardholder Information Security Program. If VISA U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating loss of this information, VISA U.S.A. may require immediate corrective action.

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, VISA may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in VISA programs.

VISA has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, VISA may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.

Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.
   To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
   - Do not access or alter compromised systems (i.e., don’t log on at all to the machine and change passwords, do not log in as ROOT).
   - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   - Preserve logs and electronic evidence.
   - Log all actions taken.
   - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
   - Be on HIGH alert and monitor all VISA systems.

2. Alert all necessary parties, including:
   - Internal information security group and Incident Response Team, if applicable
Cyber Security Incident Response Plan

- Legal department
- Merchant bank
- VISA Fraud Control Group at (650) 432-2978 in the U.S.
- Local FBI Office, U.S. Secret Service, or RCMP local detachment, if VISA payment data is compromised.

3. Provide the compromised Visa account to VISA Fraud Control Group at (650) 432-2978 within 24 hours.
   - Account numbers must be securely sent to VISA as instructed by VISA. It is critical that all potentially compromised accounts are provided. VISA will distribute the compromised VISA account numbers to Issuers and ensure the confidentiality of entity and non-public information.

4. Requirements for Compromised Entities
   All merchant banks must:
   - Within 48 hours of the reported compromise, provide proof of Cardholder Information Security Program compliance to VISA
   - Provide an incident report document to VISA within four business days of the reported compromise
   - Provide an additional incident report document to VISA no later than fourteen days after initial report (See template: Appendix C)
   - Depending on the level of risk and data elements obtained, complete within four days of the reported compromise
     - An independent forensic review
     - A compliance questionnaire and vulnerability scan upon VISA’s discretion

Steps for Merchant Banks
- Contact Visa USA Fraud Control Group immediately at (650)432-2978
- Participate in all discussions with the compromised entity and VISA USA
- Engage in a VISA approved security assessor to perform the forensic investigation
- Obtain information about compromise from the entity
- Determine if compromise has been contained
- Determine if an independent security firm has been engaged by the entity
- Provide the number of compromised VISA accounts to Visa Fraud Control Group within 24 hours
- Inform Visa of investigation status within 48 hours
- Complete steps necessary to bring entity into compliance with CISP according to timeframes described in “What to do if Compromised”
- Ensure that entity has taken steps to prevent future loss or theft of account information, consistent with the requirements of the VISA USA Cardholder Information Security Program
Discover/Experian Specific Steps:

Refer to documentation online at
American Express Specific Steps:

Refer to documentation online at https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=IDC&tabbed=breach

As a Merchant, if you know or suspect that Cardmember information has been accessed or used without authorization you must, as detailed fully in the Data Security Operating Policy:

1. Notify American Express immediately
2. Work with American Express and auditors to conduct a thorough audit of the incident
3. Provide any and all information, and follow all instructions requested by American Express regarding the incident

If you believe that Cardmember information has been compromised, contact your Client Manager or call our Customer Services Team at:

- U.S. Caribbean and Bermuda: 1-800 AXP AMEX (297-2639)

You may also notify the American Express Enterprise Incident Response Program (EIRP) by filling out the Initial Notice Form and sending it via email to EIRP@aexp.com.

You can avoid being assessed additional costs of a data incident by:

1. Notifying American Express immediately if you know or suspect your data has been compromised
2. Ensuring that you are in full compliance with the American Express Data Security Operating Policy
3. The data incident was not caused by the wrongful conduct of you or one of your employees or agents