MALICIOUS SOFTWARE PROTECTION POLICY

Version 1.0 – October 4, 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 4, 2016</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS
1. SCOPE .......................................................................................................................... 4
2. ANTI-VIRUS SOFTWARE REQUIRED FOR ALL COMPUTERS .................................. 4
3. MALICIOUS SOFTWARE SCANNING ON THE NETWORK ....................................... 4
4. ANTI-VIRUS REQUIREMENTS .................................................................................... 4
5. ANTI-VIRUS CONFIGURATION ................................................................................... 5
6. MISSOURI BOTANICAL GARDEN APPROVED SOFTWARE .................................. 5
7. ROLES AND RESPONSIBILITIES ........................................................................... 6
8. POLICY AWARENESS ................................................................................................. 6
9. RESPONSIBILITY FOR POLICY MAINTENANCE .................................................... 6
1. Scope
Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be also be implemented as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

2. Anti-Virus Software Required for all Computers
   a. All Missouri Botanical Garden Windows-based desktop computers, workstations, and laptops are required to have continually operating, approved anti-virus software with the current virus database version, unless authorized by the Vice President of Information Technology. Any computer connected to the Garden's network, whether or not Garden-owned, also must meet this requirement. This requirement is also documented in the Acceptable Information Technology Use Policy, Section 4.2, Security and Proprietary Information.
   
   b. Point of sale workstations are included in the scope of this policy and must also employ the required anti-virus programs.
   
   c. All Missouri Botanical Garden production servers, both physical and virtual, are required to have continually operating, approved anti-virus software with the current virus database version.
   
   d. Macintosh computers are not required to have anti-virus software installed because they are not typically vulnerable to malware attacks. This lack of vulnerability will be assessed annually and if considered a new risk, anti-virus software will also be installed on Macintosh computers.

3. Malicious Software Scanning on the Network
   a. Scanning for malicious software both inbound and outbound will be implemented on any firewall connected to the Internet.
   
   b. An Intrusion Detection Service will be used on the firewall connected to the Internet to detect potential zero-day malicious software behavior.
   
   c. An Intrusion Prevention Service will be used on the firewall connected to the Internet to block potential zero-day malicious software.
   
   d. An Anti-Shun device will be used between the Internet and the firewall to block traffic to and from known IP addresses of malicious activity.

4. Anti-Virus Requirements
   a. Anti-virus programs approved for use by Missouri Botanical Garden must be capable of detecting, removing, and protecting against all known types of malicious software.
Known types of malicious software include trojans, worms, spyware, adware, rootkits, ransomware, and botnets.

b. Anti-virus programs may be supplemented by additional malware protection software.

c. Anti-virus programs must be automatically loaded upon computer start and perform a scan.

d. Anti-virus programs must remain in continuous use.

e. Anti-virus programs in use must be automatically updated with the latest software version and/or the latest virus profiles upon network connection.

f. Virus scan logs for computers in-scope for PCI must be retained for one year with three months available for immediate review.

g. The latest version of the approved anti-virus program must be used.

h. The approved anti-virus program must maintain a log of scan results and report malicious software detections to a central server which can be monitored by Solarwinds Log and Event Manager.

5. Anti-Virus Configuration

Master settings for anti-virus programs used on desktop computers, workstations, laptops, servers or network equipment may only be made by Information Technology personnel authorized by the Vice President of Information Technology, Manager of User Support, or Senior Manager of Systems and Network Administration.

Anti-virus programs will be configured to disallow end users to disable or alter the program’s settings unless formally authorized by the Vice President of Information Technology.

6. Missouri Botanical Garden Approved Software

a. Anti-Virus

i. Desktop computers, workstations, laptops – ESET NOD 32

ii. Windows Servers – MacAfee Anti-Virus

iii. Email – Microsoft Cloud malware protection

b. Anti-Malware

i. Desktop computers, workstations, laptops – MalwareBytes

ii. External Firewall – Fortinet Intrusion Detection and Intrusion Prevention

iii. Internal Segmentation Firewall – Fortinet Intrusion Detection and Intrusion Prevention

iv. Internet – CyberEdge Shun appliance
7. Roles and Responsibilities
   
a. The Manager of User Support will be responsible for installation and updating of anti-virus and anti-malware software on desktop computers, workstations and laptops.

b. The Senior Manager of Systems and Network Administration will be responsible for installation and updating of anti-virus and anti-malware software and hardware on servers, firewall, networks, and external to the network.

c. The Vice President of Information Technology will be responsible for approving software programs and hardware used to support this policy and for ensuring end users are aware of the policy.

8. Policy Awareness

   All Garden computer users are required to be aware of this policy.

9. Responsibility for Policy Maintenance

   The Vice President of Information Technology is responsible for ensuring that this policy is kept current as needed.