Missouri Botanical Garden
Acceptable Information Technology Use Policy

The following policy supplements the 2010 Employee Handbook for information technology use by employees. Where conflict may occur, the Handbook is the primary governing document. For Non-Employees working at the Garden, such as contractors, consultants, students, volunteers, interns, and research associates, please refer to the Acceptable Information Technology Use Policy for Non-Employees.

1.0 Overview
Missouri Botanical Garden’s intentions for publishing an Acceptable Information Technology Use Policy are not to impose restrictions that are contrary to Missouri Botanical Garden established culture of openness, trust and integrity. Missouri Botanical Garden is committed to protecting its employees, partners and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to computer and telephone equipment, software, operating systems, storage media, laptops, tablets, printers, copiers, network accounts providing electronic mail, Internet browsing, and file sharing are the property of Missouri Botanical Garden. These systems are to be used for business purposes in serving the interests of the institution and its normal operations. Please review the 2010 Employee Handbook for further details on pages 55-61.

Effective security is a team effort involving the participation and support of every Missouri Botanical Garden employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of information technology equipment and services by employees at Missouri Botanical Garden. These rules are in place to protect the employee and Missouri Botanical Garden. Inappropriate use exposes Missouri Botanical Garden to risks including virus or malware attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to regular and part-time employees of Missouri Botanical Garden. This policy applies to all equipment that is owned or leased by Missouri Botanical Garden.

4.0 Policy
4.1 General Use and Ownership
1. While Missouri Botanical Garden's network administration desires to provide a reasonable level of privacy, employees should be aware that the data they create on the institution's systems remains the property of Missouri Botanical Garden. Because of the need to protect Missouri Botanical Garden's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Missouri Botanical Garden.
2. Policies limiting employee’s personal use of Garden equipment and services are provided in the 2010 Employee Handbook, pages 55-56.
3. For security and network maintenance purposes, authorized individuals within Missouri Botanical Garden may monitor the Garden's equipment, systems and network traffic at any time.
4. Missouri Botanical Garden reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information
1. All employees must keep passwords secure and must not exchange passwords in order to share accounts. Employees are responsible for the security of their passwords and accounts.
2. System and user level passwords must be changed at least yearly.
3. Because information contained on portable computers is especially vulnerable, special care should be exercised to maintain passwords on those devices.
4. All computers used by Garden employees that are connected to the Missouri Botanical Garden Internet/Intranet, whether owned by the employee (by exception) or Missouri Botanical Garden, shall have continually operating, approved virus-scanning software with the current virus database version, unless authorized by the Vice President of Information Technology.
5. The Garden does not allow employees to bring in personal equipment or software.
6. All computer purchases for Garden use must be purchased through the IT Department whether using unrestricted or restricted funds.
7. Garden computers must not be disconnected from the network in order to use the network cable. If you need a network cable, please call Extension 895 and request it.
8. Non-Garden-owned laptops cannot be connected to the Garden's internal network until a member of the IT Department has inspected it for viruses and determined the device has current virus software. This is required for all users with non-Garden laptops including Garden visitors. (Please call Extension 895 to establish this inspection if needed.)

Guidelines
- When you are finished using a computer, please log off or shutdown the computer.
- Never turn the computer off at the surge protector.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, because they may contain viruses or malware.

4.3. Prohibited Use
The following activities are, in general, prohibited for all employees. Some employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a computer if that computer is disrupting production services).

Under no circumstances is an employee of Missouri Botanical Garden authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Missouri Botanical Garden-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of prohibited use.

The following activities are strictly prohibited, with no exceptions:

System and Network Activities
1. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Missouri Botanical Garden or the end user does not have an active license is strictly prohibited.

2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

3. Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, malware, etc.).

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5. Use of Garden equipment, services, or facilities for the downloading, viewing, transmission, or communication of images or text consisting of threats to the safety of employees, non-employees or of ethnic slurs, racial epithets, hate speech, sexually explicit material, obscenities, or anything else that may be construed as harassing or offensive to others based on an individual’s race, color, religion, sex, national origin, citizenship, age, sexual orientation, gender identity and expression, disability, marital status, veteran status, or any other legally protected category;

6. Use of Garden electronic communication systems for pornography, violence, gambling, improper jokes, any illegal activity or for any unethical purposes. Profanity or vulgarity may not be used over Garden electronic communication systems;

7. Use of Garden electronic communication systems to solicit for commercial ventures, religious or political causes, outside organizations, or other non-Garden-related solicitations;

8. Making fraudulent offers of products, items, or services originating from any Missouri Botanical Garden account.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning unless prior notification is made to the Information Technology department and it is authorized by them.

11. Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any computer, network or account.

13. Interfering with or denying service to any computer other than the employee's own computer (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another person's computer, via any means, locally or via the Internet/Intranet.

Email and Communications Activities
1. Intentionally sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text or paging, or social networking whether through language, frequency, or size of messages.
3. Unauthorized use, or intentional forging, of email header information.
4. Solicitation of email for any other email address, other than that of the employee's own account, with the intent to harass or to collect replies.

Payment Card Industry Data Security Standards (PCI DSS) Policies
1. Sending unprotected credit card Personal Account Numbers (PAN) via unsecure end-user messaging technologies is strictly prohibited. This includes unsecure email, instant messaging, social media like Twitter or Facebook, or other unsecure communication methods.
2. Transporting or storing unprotected credit card Personal Account Numbers (PAN) via unsecure electronic media such as flash drive, CD, DVD is strictly prohibited.
3. All handling, storage and transmission of credit cardholder data must be in compliance with the Missouri Botanical Garden PCI Security Policies.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Revision History
- Revised - August 11, 2014 by Charles K. Miller, Vice President & CIO
- Revised to add PCI prohibition against sending unprotected credit card Personal Account Numbers (PAN) via end-user messaging technologies - June 30, 2015 by Charles K. Miller, Vice-President & CIO