Missouri Botanical Garden
Acceptable Information Technology Use Policy For Non-Employees

The following policy applies to the acceptable use of information technology at Missouri Botanical Garden by persons who are not employees of the Garden but require access to the Garden's information systems. These persons are referred to as Non-Employees and can include:

- Contractors and Consultants
- Interns
- Volunteers
- Research Associates
- Students, including Graduate Students
- Visiting Scientists
- Other persons who are not employees of the Garden and are performing assignments for or in collaboration with the Garden.

1. For Garden Employees please refer to the Acceptable Information Technology Use Policy.

2. 1.0 Overview
Missouri Botanical Garden's intentions for publishing an Acceptable Information Technology Use Policy for Non-Employees 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 provided to Non-Employees by the Garden, 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.

Effective security is a team effort involving the participation and support of every Missouri Botanical Garden Non-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.

3. 2.0 Purpose
The purpose of this policy is to outline the acceptable use of information technology equipment and services by Non-Employees at Missouri Botanical Garden. These rules are in place to protect the Non-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.
6. **3.0 Scope**
This policy applies to all Non-Employees of Missouri Botanical Garden who work at the Garden and utilize its information technology. This policy applies to all equipment that is owned or leased by Missouri Botanical Garden.

4. **0 Policy**

4.1 **Equipment Use**

1. **General.** The Missouri Botanical Garden may provide Non-Employees with appropriate information systems and access as needed in their collaboration with the Garden. Garden information system equipment essential to accomplishing assignments can be expensive and may be difficult to replace. Because this equipment is Garden property, all Non-Employees must use this equipment for Garden business purposes and ensure that all property provided by the Garden is kept in the best possible working condition. When using the Garden’s property, all Non-Employees must exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines.

2. **Personal Use.** Limited personal use of Garden information systems and equipment, including but not limited to telephone systems, computers, printers, Internet access and copy/fax machines, is permissible from time to time so long as it is reasonable, kept to a minimum, and not utilized in any inappropriate manner. Inappropriate or excessive personal use of the Garden’s telephone or electronic communication systems and devices will not be tolerated and may result in denial of all Garden information systems access by a Non-Employee.

3. **Software Use.** Non-Employees may have various software applications installed on their Garden-provided computers in order to facilitate their Garden-related needs. All such software must be licensed to the Garden. Software provided by the Garden is to be used only in connection with Garden business and is not to be transferred outside of the Garden without proper authorization. All software must be installed on Garden computers by Information Technology personnel unless otherwise authorized by the Vice President, Information Technology or designee. Personally owned software must not be installed on Garden computers. All software owned by or licensed to the Garden shall remain with the Garden and may not be installed on Non-Garden Equipment, without prior approval from the Vice President, Information Technology or designee.

4. **Non-Garden Laptops and other devices.** The Garden acknowledges that some Non-Employees, such as graduate students or visiting scientists, may need to use their personal equipment on Garden property to conduct assignments associated with the Garden. Also, some Non-Employees, such as contractors, may need to use equipment owned by an institution other than the Garden. All Non-Garden Computer Equipment must be pre-approved by the IT division and comply with the following before it may be connected to the Garden’s network:

- The equipment must have an operating and up-to-date anti-virus program
• The equipment must be Ethernet-compatible
• The equipment must not have any illegally copied software installed

Contact the IT Department at Extension 895 to receive approval for Non-Garden devices to connect to the Garden's network. *This does not apply to devices connected to the Garden's "public" network that is not connected to the Garden's main network and only provides access to the Internet.*

4. **Telephone Use.** The Garden recognizes that occasionally it is necessary for Non-Employees to make or receive personal telephone calls during working hours. However, personal calls during work hours can interfere with productivity and be distracting to others. Therefore, personal calls should be kept to a minimum and at a low volume, whether the calls are placed or received using Garden phones or personal cellular phones. Excessive or inappropriate personal Garden telephone usage may result in denial of access to all Garden information systems.

Non-Employees may not charge personal long-distance calls to the Garden unless specifically authorized by Garden management.

The Garden will not be liable for the loss of personal cellular phones or other Non-Garden Equipment brought to any Garden premises.

5. **Internet Use.** Access to the Internet through the Garden’s network is a privilege and requires responsible and ethical use. Limited personal use of the Internet while working at the Garden is allowed. However, Non-Employees are reminded that this Policy governs the use of all Garden information systems. Any use of the Internet must not interfere with Garden operations, be inappropriate or excessive. Non-Employees’ pathways through the Garden’s network can and may be tracked.

6. **Loss of or Damage to Garden Equipment.** The Garden may require Non-Employees who lose or cause damage to Garden equipment or property to pay the replacement costs of such lost or damaged property. Moreover, Non-Employees who are negligent in operating, fail to adequately safeguard, or inappropriately use Garden equipment and/or property may be denied access to all Garden information systems.

4.2 **No Expectation of Privacy**
1. While Missouri Botanical Garden's network administration desires to provide a reasonable level of privacy, any information, data, files, or attachments that are created, received, downloaded, stored, transmitted, deleted, or used by Non-Employees while engaged by the Missouri Botanical Garden are considered Garden property unless otherwise specified by law or written agreement with the Garden.
2. The Garden reserves the right to access, monitor, audit, search, copy, intercept, remove, or disclose any information stored on or sent through its phone system, voice mail system, or computer systems, including voice mails, e-mails, files,
software or other information stored on the network or on the Garden’s computers, for any purpose. The Garden also has the right to access any Garden information system and to block access from any Non-Garden computer, system, network, or other access point. Non-Employees should have no expectation of privacy in their electronic communications over the Garden’s systems. The Garden may take such action to maintain the integrity of its systems, network, or data; to protect the rights of authorized users of information systems; to respond to a breach or threatened breach of the integrity of any information system or of this Policy; or to address a legitimate business need or other important concern identified by the Garden.

3. Non-Employees should be aware that electronic communications, software, and other data may be copied, backed up, and/or stored by the Garden long after it is created or last accessed. Data believed to have been deleted may still be preserved in some storage medium and may be retrieved if necessary. Activity on personal computers, servers, and networking systems may be logged by administrative software included on such equipment, and these logs may be monitored and reviewed by system administrators or discovered in legal proceedings. These copies, backups, activity logs, and other records may persist on Garden information systems after a Non-Employee’s affiliation with the Garden ends. In addition, defects, breaches, and limitations of the information systems may compromise the confidentiality of users’ information or materials.

4. Finally, while the Garden may treat some information systems as confidential, the Garden cannot guarantee the security of those information systems against unauthorized access or disclosure.

4.3 Confidential Information

1. All non-public or unpublished information relating to the Missouri Botanical Garden and its visitors is confidential. Other examples of confidential information include, but are not limited to, the Garden’s objectives, processes/procedures, information about customer and visitor relationships, employee and member information, and technology systems.

2. All Non-Employees who use the Garden’s data systems must safeguard Garden confidential information, whether generated internally or acquired from other sources, and use it only in the performance of their assignments. Confidential information must not be removed from the Garden without authorization of the department head responsible for the information. Anyone who discovers a violation of this policy should immediately notify his/her sponsoring manager or the Information Technology department. This policy is intended to alert Non-Employee data users to the need for discretion at all times and is not intended to inhibit normal business communications.

4.4 Confidentiality and Monitoring

1. Because of the need to protect Missouri Botanical Garden’s network, Garden management cannot guarantee the confidentiality of information stored on any network device belonging to Missouri Botanical Garden.
2. 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.

3. Missouri Botanical Garden reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4. Authorized employees of the Garden, including Information Technology staff charged with the daily administration of the Garden’s information systems, may:
   • Take all reasonable steps necessary to preserve the availability and integrity of information systems, including blocking any user's access to them.
   • Reject or destroy e-mail messages, e-mail attachments, and other files suspected of being spam or containing malicious code, such as viruses, worms and botnets
   • Exercise administrative authority over networks, systems, or software in order to grant users access to read, write, edit, or delete information in files or databases, to establish security controls and protection for information systems, or to address claims that intellectual-property or other rights have been violated
   • Employ a variety of security monitoring devices and tools to identify misuse or unauthorized use of information systems
   • With the approval of the Vice President, Information Technology, temporarily shut off the Garden's Internet connection, servers, or services, without prior notice, in order to protect Garden systems, data, and users or to protect other important interests of the Garden
   • Temporarily or permanently terminate users' use of information systems to investigate or remedy any threat to the information systems or violation of this Policy; and,
   • Exercise administrative rights over certain information systems, if those rights are delegated to the Information Technology staff.

7. 4.5 Security and Proprietary Information

1. User IDs and passwords are the primary method of authenticating users of the Garden's information systems. They help to prevent unauthorized access to information systems or any restricted information found within them. All computer passwords are considered to be confidential and private and must not be shared. All Non-Employees must keep passwords secure and must not exchange passwords in order to share accounts. Non-Employees are responsible for the security of their passwords and accounts. However, passwords do not confer any right or reasonable expectation of privacy upon any user of the Garden’s information systems.

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 Non-Employees that are connected to the Missouri Botanical Garden Internet/Intranet, whether owned by the Non-Employee (by exception) or by 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 encourages Non-Employees to not bring in personal equipment or software. However, the Garden understands that visiting students, scientists, research associates and others may need to utilize personal laptops or other devices to conduct their work at the Garden. In order to connect these “visiting devices” to the Garden's network for access to shared disk drives or printers, a network access request must be submitted to the IT department so a network user id and password can be assigned. Devices without a Garden login/password may only access the Internet.

6. 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.)

7. All computer purchases for Garden use must be purchased through the IT Department whether using unrestricted or restricted funds.

8. Garden computers must not be disconnected from the network in order to use the network cable. If a network cable is needed, please call Extension 895 and request it.

Guidelines

• When you are finished using a Garden computer, please log off or shutdown the computer. Never turn the computer off at the surge protector.

• Non-Employees must use extreme caution when opening e-mail attachments received from unknown senders, because they may contain viruses or malware.

8. 4.6 Prohibited Use

The following activities are, in general, prohibited for all Non-Employees and employees.

Under no circumstances is a Non-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:

9.

10. Prohibited 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 Garden management should be consulted prior to export of any material that is in question.

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

4. Revealing your Garden 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 Garden network communication. Security breaches include, but are not limited to, accessing data of which the Non-Employee is not an intended recipient or logging into a Garden server or account that the Non-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 Non-Employee's Garden-assigned computer unless this activity is a part of the Non-Employee's normal job/duty.

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

13. Interfering with or denying service to any computer other than the Non-Employee's own computer (for example, denial of service attack).
14. Using any Garden-assigned 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.

11. Prohibited Email and Communications Activities

1. Intentionally sending unsolicited email messages from a Garden-assigned email address, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material unless authorized by Garden management.
2. Any form of harassment via Garden email, telephone, text or paging, or Garden-assigned social networking whether through language, frequency, or size of messages.
3. Unauthorized use, or intentional forging, of Garden email header information.
4. Solicitation of email for any other email address, other than that of the Non-Employee's own Garden-assigned email 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

Failure to comply with these requirements could result in damage to the Garden and if damage does occur, the Non-Employees involved may be held liable for the damages. The Garden may restrict or deny access to its network or facilities by any Non-Employee who fails to comply with these requirements.

6.0 Revision History

- Created 2011 by Charles K. Miller, Vice President & CIO
- Revised August 11, 2014 by Charles K. Miller, Vice President & CIO
- Revised to add PCI policies to prohibit sending credit card Personal Account Numbers (PAN) via end-user messaging – June 30, 2015 by Charles K. Miller, Vice President & CIO