Missouri Botanical Garden Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Missouri Botanical Garden's entire corporate network. As such, all Missouri Botanical Garden employees and staff (including contractors and vendors with access to Missouri Botanical Garden systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Missouri Botanical Garden facility, has access to the Missouri Botanical Garden network, or stores any non-public Missouri Botanical Garden information.

This policy extends the Acceptable Information Technology Use Policy and the Acceptable Information Technology Use Policy for Non-Employees.

4.0 Policy
4.1 General
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a yearly basis.
- All production system-level passwords must be part of the strongly encrypted Information Technology administered global password file.
- The user-level network and email password initially assigned to a new user must be changed on first use.
- All user-level network and email passwords must contain a minimum of 7 characters and include both alphabetic and numeric characters.
- More than 6 failed password attempts will result in the user's account being blocked and will require contacting IT User Support at extension 895 to be reactivated.
- All user-level network and email passwords will automatically expire after 3 months and must be changed at least that frequently. A new password cannot be the same as any of the prior five passwords.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All user-level and system-level passwords must conform to the guidelines described below.
4.2 Guidelines
A. General Password Construction Guidelines

- Passwords are used for various purposes at Missouri Botanical Garden. Some of the more common uses include: user level accounts, database applications, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:
- A poor, weak password contains less than seven characters.
- A poor, weak password is a word found in a dictionary (English or foreign).
- A poor, weak password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

**MBG network access passwords are required** to contain at least three of the following categories:
1. Lower case letters (a-z)
2. Upper case letters (A-Z)
3. Numbers (0-9)
4. Punctuation characters (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Are at least seven alphanumeric characters in length. **MBG network access passwords are required to be at least 7 characters.**
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down, tape to desk drawer, underneath keyboard or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!
B. Password Protection Standards

- Do not use the same password for Missouri Botanical Garden accounts as for other non-Missouri Botanical Garden access (e.g., personal ISP account, online banking, benefits, etc.). Where possible, don't use the same password for various Missouri Botanical Garden access needs. For example, select one password for the database applications and a separate password for personal computer systems.

- Do not share Missouri Botanical Garden passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Missouri Botanical Garden information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your manager
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact the Vice President, IT at extension 419 or IT User Support at extension 895.

Do not use the "Remember Password" feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smartphones, tablets or similar devices) without encryption of the file.

If an account or password is suspected to have been compromised, report the incident immediately to IT User Support and change all passwords.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- must support authentication of individual users, not groups.
- must not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
5.0 Enforcement
As also declared in the *Garden Employee Handbook* and the *Acceptable Information Technology Use Policy*, any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Revision History
Revised August, 2014
Revised December 1, 2015
Revised October 18, 2016
Revised November 1, 2016