

UGA Password Standard

1.0 Overview

This document describes the acceptable means for password construction, protection, and maintenance.

2.0 Password Construction

Passwords must have a minimum of eight alphanumeric and special characters; if a particular system will not support eight characters, then the maximum number of characters allowed must be used. Passwords will not be composed of one or more dictionary words in any language, human or artificial.

One method to create an easily remembered password is to base it upon the first character of a phrase such as, "I Went Downtown To Buy 3 Items Today." The password would be Iwdtb3iT. As this is a known password do not use it.

More password construction guidelines can be found in Appendix A of this document, *Password Guidelines*.

3.0 Password Management

Creating an effective password is not possible if the password is not properly managed.

3.1 Password 'Storage'

- Passwords should be memorized.
- Passwords must not be stored in a manner which allows unauthorized access. For example, writing the password down and attaching it to the monitor or placing it in a desk drawer or under the keyboard is unacceptable.
- Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.
- Computers must not be configured to login without a password. Exceptions may be granted for specialized devices such as kiosks which have extremely restricted accounts. Whenever possible, computer labs should be designed to authenticate each user individually for accountability purposes.

3.2 Password Aging

Users must change their passwords at least twice (2x) per year with the new password incorporating at least 3 changed characters.

3.3 Limit damage from compromised passwords

Care must be taken to prevent the compromise of one username/password from compromising multiple systems or resources. For example, users must not use the username and password combination from any non-UGA account as the username and password for their UGA MyID. This is especially important if the non-UGA system does not use encrypted authentication.

4.0 Password Transmission

Passwords must not be transferred or shared with others unless authorized to do so.

4.1 Electronic

Passwords must not be transferred electronically over the Internet using insecure methods. Insecure methods include Post Office Protocol (POP), Internet Mail Access Protocol (IMAP), File Transfer protocol (FTP), Hyper-Text Transfer Protocol (HTTP), and Telnet.

4.2 Written

When it is necessary to disseminate passwords in writing, the recipient will take measures to protect the written password from unauthorized access. For example, after memorizing the password, one must destroy the written record.

4.3 Oral

When transmitting a password orally, take measures to ensure that the conversation is not overheard by unauthorized individuals.

5.0 Additional Password Considerations

5.1 System Administrators

System administrators, or those serving that role, may need to create and disseminate passwords to others. Whenever possible, use a method of password creation that provides the password only to the intended end-user.

System administrators must harden their systems to deter password cracking:

- An automated method to mitigate “brute force” password attacks must be used. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts

from that location, or at minimum alert the system administrator in real-time that an attack is underway so that manual action can be taken.

- Logging must be set up to record all failed login attempts and preferably successful attempts as well.

5.2 Application Developers

- Application developers must develop applications using secure authentication methods, whenever possible.
- Application developers should avoid creating applications which store passwords. If password storage cannot be avoided, application developers must ensure that applications do not store passwords in clear text or employ a readily decrypted form.
- Applications should support unique logins. Additionally, role management (e.g. system administrators, network administrators) should not require password sharing.
- Using the UGA MyID for authentication is preferable to creating another unique ID for users under most circumstances, but only when the MyID is used in a secure fashion, i.e., no unencrypted logins.

6.0 Events Necessitating Password Change

If any of the following events occur, a password change will be mandatory:

- Unauthorized password discovery or usage by another person
- System compromise (unauthorized access to a system or account).
- Insecure transmission of a password, for example via email or instant message. (Even an email transferred via secure Post Office Protocol (POP) or Secure Internet Message Access Protocol (S-IMAP) could be compromised at the Simple Mail Transport Protocol (SMTP) level or read while in your inbox- change the password anyway.)
- Accidental disclosure of password to an unauthorized person
- Replacement of account user with another individual requiring access to the same account
- Password is provided to IT support staff in order to resolve a technical issue (It is strongly recommended that IT support staff request an end-user password as a last resort.)
- A password is provided to the end-user and the system administrator knows the

Created: 3/23/2006 [pm]
Revised On:

password. For example, the system administrator provides a new account password or has to reset an account password.

Appendix A. Password Guidelines

Different computing systems place different limitations on password construction. The following applies to all computing systems, whether or not the system enforces these limitations:

Unacceptable Methods to Create a Password:

- Do not use dictionary or actual words. Non-English words are no more secure than English words. (If you accidentally use a tiny dictionary word like “I”, “a”, “an”, or “if” in an otherwise secure password, that is fine.)
- Do not use words or numbers associated with you. Examples include:
 - Social security numbers
 - Names, family names, pet names
 - Birthdays, phone numbers, addresses
 - Avoid using your login name or any variation of it as your password. If your login is ‘fredrick’, do not use substitution or letter reordering. Examples would be ‘fr3dr1ck’, where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- Do not use the same character for the entire password (e.g., '11111111') or use fewer than five unique characters.
- Do not use common letter or number patterns for your password (e.g., '12345678' or 'abcdefgh').
- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).
- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

Password cracking tools are sophisticated and are able to crack passwords that are created using these unacceptable methods.

Acceptable Methods to Create a Password:

- Use a minimum of 8 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.
- Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use letters from a passphrase or sentence, e.g., “One ring to rule them all, one ring to bind them” results in the password of “1R2rtA,or2Bt” by using the first letter, capitalization, and some substitution.
- Use mixed case (upper & lower)
- Use punctuation symbols (Ex: _-+ = ! @ % * & ’ : , . /)