Password Protection Policy

Responsible Office: Information Technology Support & Services
Originally Issued: December 2005
Revised: Not applicable

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 critical GHSU resources. As such, all GHSU faculty, staff and students (including contractors and vendors with access to GHSU 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 GHSU facility, has access to the GHSU network, or stores any non-public GHSU information.

4.0 Policy

IT Support Professional

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed every 90 days.
- All systems administrative-level passwords for production environments must be part of an ITSS administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Where SNMP (System network management protocol) 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. A keyed hash must be used where available (e.g., SNMPv3).

General Users

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 90 days.
- Passwords must not be included in email messages or other forms of electronic communication.
- Passwords must be at least 8 characters in length.
- All user-level and system-level passwords must conform to the guidelines described below.

5.0 Guidelines

General password construction guidelines are used for various purposes at GHSU (i.e. user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins). It is important that everyone be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password can be found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, 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, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

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!

Password protection standards

- Change passwords at least once every 90 days.
- Do not write down passwords
- Do not store passwords on-line without encryption.
- Do not use the same password for GHSU accounts as for other non-GHSU access (e.g., personal ISP account, on-line banking, email, benefits, etc.).
- Do not share GHSU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential GHSU information.
- 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 the boss
- 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
- Don’t use the “Remember Password” feature of applications (e.g., Groupwise, Instant Messenger, Internet Explorer, Mozilla).

If someone demands a password, refer them to this document or have them call the IT Service Desk.

If an account or password is suspected to have been compromised, report the incident to ITSS Security Administration and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by ITSS Security Administration or its delegates. If a password is guessed or cracked during one of these scans, the incident will be documented and the user will be required to change it. Repeated offenses will be subject to appropriate disciplinary action as outlined in the Employee Rules of Conduct.

Please visit the following page for more password creation guidelines.
http://policy.georgiahealth.edu/2010/09/23/password-protection-policy/

6.0 Application Development Standards

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

Applications:

- Should support authentication of individual users, not groups.
- Should 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.
- Should support 802.1x, TACACS+, RADIUS, secure LDAP retrieval, wherever possible.

7.0 Related Documents

Information Security Glossary of Terms to Know

This entry was posted in *Administrative*, *Information Technology Support & Services* and tagged *password*, *password protection*, *security*, *strong password*. Bookmark the *permalink*. Both comments and trackbacks are currently closed.

« *Electronic Mail Retention, Backup, and Recovery Policy* *Remote Access Policy* »