Policy # 56004

INFORMATION TECHNOLOGY PASSWORD POLICY

Effective Date: June 19, 2009 **Review Date: January 25, 2022**
Responsible Office: Information Technology Center
Division: Operations

I. PURPOSE

The purpose of this policy is to establish a standard for the usage of strong passwords, the protection of those passwords, and the frequency of change according to the Louisiana Office of Information Technology's password policy IT_POL_1-08 and standard IT_STD_1-01.

II. STATEMENT OF POLICY

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 Grambling State University entire corporate network. As such, all Grambling State University employees and students (including contractors and vendors with access to Grambling State University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Employees, students, contractors and vendors are responsible for accounts (or any form of access that supports or requires a password) on any GSU Information Technology network.

A. General

All passwords shall be constructed and implemented according to the following criteria:

1. Passwords must be treated as confidential information.
2. Passwords shall be routinely changed every 2 years or less.
3. Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups;stored procedures)are not subject to the routine change specified here. Service account passwords must be changed with changes in personnel (termination, change in duties, transfer, etc.).
4. Owners of systems that maintain mission critical and/or confidential information shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse;
5. Passwords should not be anything that can be easily associated with the account owner such as: user name, social security number, UIN, nickname, relative's name, birth date, telephone number, etc.;
6. Passwords should not be dictionary words or acronyms regardless of language of origin and must be unique;
7. Stored passwords shall be encrypted;
8. Passwords shall never be transmitted as plain text;

9. There shall be no more than seven tries before a user is locked out of an account.
10. Security tokens (e.g., Smartcard) must be returned when there has been a change in job duties which no longer require restricted access, or upon termination of employment;
11. If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s);
12. Users shall not circumvent password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always enter "no" when asked to have a password "remembered";
    a. Exceptions may be made for specific applications (like automated backup) with the approval of the information resource owner. In order for an exception to be approved, there must be a procedure for the user to change passwords.
13. Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device;
14. Forgotten passwords shall be replaced, not reissued;
    a. Procedures for setting and changing GSU user passwords include the following:
        i. The user must verify his/her identity before the password is changed;
        ii. The password must be changed to a "strong" password
        iii. The user must change password at first log on – where applicable.
15. Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service;
    a. Automated password generation programs must use nonpredictable methods of generation, should be unique; and,
    b. Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.
16. All servers and workstations shall have passwords that conform to this ITC Password policy.

B. Password Protection Standards

Do not use the same password for Grambling State University accounts as for other non-University access (e.g. personal ISP account, option trading, benefits, etc.). There will be three attempts after the third attempt the account will be locked and users must submit a work order via the GSU Track It Help Desk for assistance. Where possible, don't use the same password for various Grambling State University access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and an Oracle account.

Do not share Grambling State University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

If an account or password is suspected to have been compromised, report the incident to Information Technology Center and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the Information Security Officer or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

III. REVISION/REVISED HISTORY

September 2023 - Revision
January 2023 - Revision
February 2011-Revision
June 19, 2009-Effective Date