GRAMBLING
STATE UNIVERSITY

Policy # 56004

INFORMATION TECHNOLOGY PASSWORD POLICY

Effective Date: June 19, 2009 **Revised Date:** May 22, 2025
Responsible Office: Information Technology Center
Division: Finance

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.

Grambling State University is accredited by the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) to award associate, baccalaureate, master's, and doctorate degrees. GSU also may offer credentials such as certificates and diplomas at approved degree levels. Questions about the accreditation of GSU may be directed in writing to the Southern Association of Colleges and Schools Commission on Colleges at 1866 Southern Lane, Decatur, GA 30033-4097, by calling (404) 679-4500, or by using information available on SACSCOC's website (www.sacscoc.org)

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

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
2. All production system-level passwords must be part of the Information Technology Center administered global password management database.
3. In alignment with NIST SP 800-63B guidance, user-level passwords are set to expire every 365 days. NIST recommends that passwords only be reset when there is evidence of compromise or after a defined period, such as annually.
4. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

5. 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. A keyed hash must be used where available (e.g., SNMPv2).
6. Grambling State University utilizes Microsoft Azure for user authentication, meaning computer and email passwords are synchronized and the same across both platforms.

---

7. All user email accounts are protected by Multi-Factor Authentication (MFA) to enhance security and prevent unauthorized access.
8. Users can change and manage their passwords via the GSU Portal, accessible through QuickLaunch.

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 Banner 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.

C. Additional Standards

Password Length and Complexity: Per CMMC standards, passwords must be a minimum of twelve (12) characters

III. REVISED/REVIEWED

- May 22, 2025