



## 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**

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. All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every thirty days.
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).

**INFORMATION TECHNOLOGY 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 Information Technology Center Security Administrator 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**

February 2011-Revision

June 19, 2009-Effective Date