GEORGIA SOUTHERN UNIVERSITY

PASSWORD SECURITY STANDARDS

Area:	Information Technology Services	Number:	
Applies to:	University Community	Issued:	August 6, 2012
Sources:	USG IT Handbook	Revised:	March 8, 2021
		Reviewed:	
Policy Owner:	Chief Information Officer	Page(s):	3

I. Purpose

University System of Georgia Information Technology Handbook Section 2.9.3 established that the Board of Regents shall rely on the Chancellor, the presidents of all USG institutions, and their chief information officers to develop, adapt, and administer the information technology methods and procedures for promoting efficiency of operations and the advancement of learning. Further, it is the responsibility of each institution to establish a standard for protecting passwords and the frequency of change for such passwords to mitigate compromise of sensitive information.

II. Policy Statement

Georgia Southern University has established minimum guidelines for password security to promote and protect efficient operations and the learning environment. All users of University systems/hardware/software are required to follow these University security standards. If an account or password is suspected of being compromised, the incident must be reported immediately to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or designee. Failure to maintain required password security or to report suspected security compromises may result in disciplinary action up to and including dismissal, and/or legal action. Any known violation of this policy is to be reported to the CIO or his/her designee.

This security standard applies to all users (employees, contractors, vendors, and other parties) of Georgia Southern University information technology systems or data, and all are expected to understand and abide by the Standard.

III. Exclusions

There are no exceptions to this policy.

IV. Procedures / Standard

A. All passwords will be treated as sensitive, confidential information and must not be shared with anyone including but not limited to administrative assistants, system administrators and helpdesk personnel.

B. Passwords to any computing resource must only be issued to authorized users. Password recipients are responsible for protecting the confidentiality of their password(s).

C. Passwords must not be stored in clear text. Cryptography must be used to protect the stored information.

D. Users must not write passwords down or store them anywhere in their office or publicly. Electronically stored passwords must utilization encryption on any computer system (including tablets or similar devices).

E. All user- level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days.

F. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from other accounts held by that user.

G. Passwords must be changed from their default values.

H. Passwords must not be inserted into email messages or other forms of electronic Communication unless encrypted.

I. 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.

J. If an account or password is suspected of being compromised, the incident must be reported to the appropriate administrator or in accordance with local incident response procedures.

K. Temporary or “first use” passwords (e.g., new accts or guests) must be changed upon first logon the authorized user accesses the system and have a limited life of inactivity before being disabled.

L. Passwords must be constructed with the following characteristics:

   1. Are at least fourteen characters in length (longer is better)
   2. Must contain the following four types of characters:
      a. English upper case (A-Z)
      b. English lower case (a-z)
      c. Numbers (0-9)
      d. Non-alpha special characters ($, !, %, ^, …)
   3. Must not contain the user’s name or part of the user’s name
   4. Must not contain easily accessible or guessable personal information about the user or user’s family (such as birthdays, children’s names, addresses etc.).

M. System/Workstation Password settings must have the following password settings:

   1. Password History: 8 remembered
   2. Minimum Password Age: None
   3. Maximum Password Age: 180 days
   4. Password must meet complexity: Yes (see section L.2. above)
   5. Account Lockout Duration: 15 minutes
   6. Account Lockout Threshold: 5
   7. Reset account lockout counter after 15 minutes

N. Password Protection

   1. Do not use the same password for Georgia Southern accounts as for other non-Georgia Southern access (e.g., personal ISP account, option trading, benefits, etc.).
   2. Do not share Georgia Southern passwords with anyone. This includes, but is not limited to peers, subordinates or supervisors.
   3. All passwords are to be treated as sensitive, Confidential Georgia Southern information.
   4. Concerning your password(s):
      a. Don't reveal a password over the phone to ANYONE
      b. Don't reveal a password in an email message
      c. Don't reveal a password to the boss
      d. Don't talk about a password in front of others

e. Don't hint at the format of a password (e.g., "my family name")
f. Don't reveal a password on questionnaires or security forms
g. Don't share a password with family members
h. Don't reveal a password to co-workers while on vacation

5. If someone demands a password, refer them to this document or have them call someone in the Information Security Department.
6. Do not use the "Remember Password" feature of applications (e.g., Google, Web forms, etc.).

If an account or password is suspected to have been compromised, report the incident to the HelpDesk or Information Security and change the password.

Enforcement

The CIO is responsible for enforcement of this standard. Violations of this standard could result in serious security incidents involving sensitive university, state, federal and privacy data. Violations of this policy can lead to disciplinary action up to and including dismissal, and/or legal action. Any known violation of this policy is to be reported to the CIO or his/her designee.

These standards will guide periodic security reviews, as well as audits by Internal Audit, Risk & Compliance.