Augusta University
Policy Library

Password Protection Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT
This policy applies to all account holders of Augusta University (AU) owned or managed information technology, hereinafter referred to collectively as "AU". This policy applies to all duties of AU employees and staff performed within the scope of their employment at any site of the AU. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive information (SEI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to SEI, PHI, PCI or ePHI.

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to information systems, services and applications unless specifically designated as a public access resource.

All AU workforce members (including but not limited to contractors and vendors with access to information systems) are responsible for taking the appropriate steps to select and secure their passwords. Passwords should never be shared with anyone.

Passwords are an important aspect of computer security. Poorly chosen and unchanging passwords could lead to inappropriate or unauthorized access to enterprise information resources, which could impact data integrity and availability.

This policy adheres to or exceeds the standards found in the University System of Georgia, USG IT Handbook – 5.12 Password Security.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☒ Visitors
☐ Other: *Any individual or entity with access to enterprise information technology*

PROCESS & PROCEDURES
Password Creation
All user-level and system-level passwords must conform to the current Password Configuration Standards.

- Users must use a separate, unique password for each of their work-related accounts.
- Users may not use any work-related passwords for their own, personal accounts.
- Administrative and 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 to access system-level privileges. In addition to single sign on, multi-factor authentication must be used across the institution.

Access to all AU information systems and applications used to process, store, or transfer data shall require, at minimum, the use of standard passwords or other authentication mechanisms.

Standard passwords shall be constructed with the following characteristics:

- Be at least eight (8) characters in length
- Must contain characters from at least two of the following four types of characters:
    - English upper case (A – Z)
    - English lower case (a - z)
    - Numbers (0 – 9)
    - Non-alphanumeric special characters ($, %, ^, …)
- Must not contain the user's name or part of the user's name
- Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.

Note: An eight-character password is acceptable if "account lockout" is enabled and set to lock or disable the account after five unsuccessful or failed login attempts. Eight-character passwords must adhere to all the characteristics noted above.

Password Protection

- Each user of an information system shall be assigned a unique user identification and password
- If you suspect your account and/or password has been compromised, report the incident to IT Cybersecurity Office and change the password (72CYBER@augusta.edu, 706-722-9237)
- Do not write down passwords
- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential AU information.
- Do not store passwords without encryption systems in place.
- Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
- Do not use the "Remember Password" feature of applications (for example, web browsers).

Application Development

Application developers must ensure that their programs contain the following security precautions:

- AU IT workforce will enable applications to automatically enforce the password creation and password change requirements through technical policy creation.
- Applications, when it is available, will ensure that "first use" password banners or notifications are delivered to the users and enforce a change of password from the "first use" password supplied to the user.

- New passwords will be at least 4 characters different from current passwords and for at least 6 historical passwords.
- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must 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.
- Use SSO authentications when technically feasible.
- Multi-Factor Authentication (MFA) must be enabled for applications across the institution.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

REFERENCES & SUPPORTING DOCUMENTS
Password Authentication Standard
USG IT Handbook https://www.usg.edu/information_technology_services/it_handbook/

RELATED POLICIES
Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021