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), Payment Card Industry (PCI) 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*

DEFINITIONS
Refer to the Augusta University Cybersecurity Charter Policy for applicable definitions.

Office of Legal Affairs Use Only
Executive Sponsor: VP, Information Technology
Next Review: 5/2030

PROCESS & PROCEDURES

I. Password Creation

1. All user-level and system-level passwords must conform to the current Password Configuration Standards.
   a. Users must use a separate, unique password for their work-related accounts.
   b. Users may not use any work-related passwords for their own personal accounts or devices.
   c. 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.
   d. 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 approved authentication mechanisms (such as authentication tokens).

2. **Standard Passwords** shall be constructed with the following characteristics:
   a. Be at least twelve (120 characters in length.
   b. **Must** contain character from at least three of the following four types of characters:
      1) English upper case (A – Z)
      2) English lower case (a – z)
      3) Numbers (0 – 9)
      4) Non-alphanumeric special characters ($, %, ^, …)
      5) Users should create a long multiword “passphrase” rather than a short and complex combination of letters, symbols, and numbers.
   c. Must not contain the user’s name or part of the user’s name.
   d. Must not contain easily accessible or guessable personal information about the user or user’s family, such as birthdays, children’s names, addresses, etc.
   e. Must not be a predictable sequence of patterns of keystrokes on the keyboard.

3. **Service and Administrator Accounts** must follow the standard complexity requirements for user accounts and the following length requirements:
   a. Administrator-level account (privileged account) passwords shall be at least 20 characters in length.
   b. Service and Administrator accounts shall be separate accounts and not elevated user-accounts.
   c. Passwords for non-interactive/service accounts shall be at least 30 characters.

4. **Password Change Policy**
   a. All passwords shall be changed upon signs of possible compromise or loss.
   b. User-level account passwords shall be changed every 365 days if protected by MFA and every 180 days if not protected by MFA.
   c. Service and Administrator account passwords shall be changed every 365 days if protected by MFA and every 180 days if not protected by MFA.

d. Passwords for non-interactive/service accounts shall be changed every 365 days if protected by MFA and every 180 days if not protected by MFA.
e. A twelve-character password is required if "account lockout" is enabled and set to lock or disable the account after five unsuccessful or failed login attempts. Twelve character passwords must adhere to all the characteristics noted above.

5. **Password Protection**
   a. If a user suspects their account and/or password has been compromised, or user gives or exposes it to someone else, the user must change it immediately.
   b. Users must report any suspected or know compromise of a password immediately to IT Cyber Defense at 72CYBER@augusta.edu or 706-722-9237.
   c. Do not write down passwords or store them in an unencrypted file.
   d. Passwords must not be shared with **anyone**, including supervisor, family members, administrative assistants and coworkers. All passwords are to be treated as sensitive, confidential AU information.
   e. Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
   f. Do not use the "Remember Password" feature of applications (for example, web browsers) as this may result in unauthorized account access. If access to a device is achieved, all saved passwords are compromised, potentially compromising all user accounts. This is especially concerning for lost or stolen devices.
   g. Account lockout, or other rate-limiting mechanisms must be enabled to lock or disable the account after five unsuccessful or failed login attempts. Temporary lockouts are permitted provided the lockout period is longer than ten minutes.
   h. Each user of an information system shall be assigned a unique user identification and password.

II. Multifactor Authentication (i.e. DUO)

1. Multifactor Authentication (MFA) must be enabled for applications across the institution where technically feasible to reduce the risk of account compromise by mitigating the weakness of single-factor authentication. Users are required to use AU provided MFA options (i.e. DUO, YubiKey, etc.) systems, products, or service that do not support MFA, must be reviewed by appropriate information technology teams, and follow the Risk Acceptance process.

2. When single-sign-on is implemented, MFA must also be implemented.

3. Use single-sign-on (SSO) authentications with technically feasible.

4. When single-sign-on is implemented, MFA must also be implemented.

5. Users must not accept MFA prompts they did not initiate. If user accepts an MFA prompt they did not initiate or wrongly accepts, it must be reported immediately to IT Cyber Defense at 72CYBER@augusta.edu or 706-722-9237.

6. Users are required to complete both authentication (two-factor/multi-factor) steps for access to computers and AU-managed websites, ensuring an added layer of security.

7. MFA Authenticators (App, Phone, Tokens, etc.) should be considered protected information and follow the same provisions listed with "Password Protection" above.

8. Authenticators should be configured only on devices which are owned and maintained by the account holder and **not shared with other individuals**. MFA should no be configured on another person's device and another person should never accept an MFA push for another user to include phone prompts.

9. Cyber Defense will submit an exception to policy (ETP) memorandum to the USG Chief Information Security Officer (CISO) for any applications without Multifactor Authentication enabled.

III. Application Development

1. Application developers must ensure their programs contain the following security precautions:
   a. AU IT workforce will enable applications to automatically enforce the password creation and password change requirements through technical policy creation.
   b. Applications, when it is available, will ensure that "first use" password banner or notification are delivered to the users and enforce a change of password from the "first use" password supplied to the user.
   c. New passwords will be at least 4 characters different from the current passwords and for at least 6 historical passwords.
   d. Applications must support authentication and individual users, not groups.
   e. Applications must not store passwords in clear text or in any easily reversible form.
   f. Applications must not transmit passwords in clear text over the network.
   g. 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.
   h. Use SSO authentications when technically feasible.
   i. Any application that does not meet all the requirements must receive an exception to policy approved by the Augusta University Chief Information Officer.

IV. Violations of this policy 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

RELATED POLICIES
Intentionally left blank.

APPROVED BY:
Interim Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/7/2025

President, Augusta University Date: 5/14/2025