Augusta University
Policy Library

Password Protection Policy

Policy Owner: Information Technology Support and Services

POLICY STATEMENT
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 faculty, staff and students (including 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. A poorly chosen and unchanging password could lead to inappropriate or unauthorized access to enterprise information resources, which could impact data integrity and availability.

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:

DEFINITIONS
Intentionally left blank.

PROCESS & PROCEDURES
- If you suspect your account and/or password has been compromised, report the incident to ITS Information Security Office and change all passwords
- Do not write down passwords
- Do not reuse a password
- Do not store passwords without encryption.
- Do not use the same password for Augusta University accounts as for other non-Augusta University access (e.g., personal ISP account, on-line banking, email, benefits, etc.).
- Do not share Augusta University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Augusta University information.
  - Don’t reveal a password over the phone to ANYONE
  - Don’t reveal a password in an email message
  - Don’t reveal a password to your supervisor
  - Don’t talk about a password in front of others
  - Don’t hint at the format of a password (e.g., “my family name”)
• Don’t reveal a password on questionnaires or security forms
• Don’t share a password with family members
• Don’t reveal a password to co-workers while on vacation
• Do not use your username, first or last name in the password
• Don’t use the “Remember Password” feature of applications (e.g., Email, Instant Messaging, Web browser, etc.).

REFERENCES & SUPPORTING DOCUMENTS
• Password Standard

RELATED POLICIES
Intentionally left blank.

APPROVED BY:
President, Augusta University and CEO, AU Health System Date: 06/13/2017