Policy Number: VI.03
Policy Level: Operating Policy
Originally Issued: December 4, 2013
Revised: April 13, 2016
Reviewed: May 15, 2018
Reviewed: June 8, 2020
Reviewed: November 3, 2022
Policy Owner: Provost/VP for Academic Affairs
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6

Password Management and Use

I. Policy Statement and Purpose

In accordance with state and Federal laws, and the University's *Information Systems Security Policy*, this policy establishes the standards for password management and use at Athens State University. This policy outlines acceptable and unacceptable practices in reference to the use and management of passwords. The standards established in this policy are based upon best practices used in higher education and follow the ISO 27001 security standards.

This policy applies to all Athens State University students, faculty, staff, and guests as well as vendors/contractors, visitors, and all others conducting official business or participating in any activity with the University. This policy applies to all fixed and portable computer and telecommunications equipment owned and issued by the University or used on the University network.

This policy also applies to third parties acting in a similar capacity to our employees whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with the University's information security policies.

II. Password Policies and Standards

A poorly constructed password may result in the compromise of an individual account or even the entire Athens State University network. All students, employees, contractors, and vendors with access to Athens State University systems are responsible for taking the appropriate steps as outlined in this policy to select and secure passwords. Therefore, passwords are necessary to protect access to user accounts.

Strong Passwords

The University will require strong passwords on all accounts that access computing and network resources to the extent that the enforcement and management of such passwords is supported by individual systems.

Password Compromises

Suspected password compromises must be reported to the Help Desk in Information Technology Services immediately. Password compromises require that all account passwords of the user to be reset and the compromise circumstances reviewed.

Password Privacy

Users should not comply with a demand to share a password. Never share a password with anyone, including Information Technology Services (ITS) staff. Should issues arise that require Information Technology Services to access an account, the password will be reset with the knowledge of the user. After issues are resolved, the user will be requested to reset the password.

Password Protection Standards

The following password protection standards are to be followed by all groups and individuals referenced in Section I of this policy:

a. Passwords should not be inserted into email messages or other forms of electronic communication.
b. Passwords should not form a word in any language, slang, dialect, or jargon.
c. Passwords should not include personal information including family names, birthdates, addresses, SSNs, etc.
d. Do not use the same password for Athens State accounts as for other non-Athens State access (e.g., personal ISP account, option trading, benefits, etc.).
e. Do not share Athens State passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential.
f. Do not construct passwords that contain a word/phrase in any language, slang, dialect, jargon, etc. or be based on personal information, names of family, birthdates, etc.
g. Construct and use strong passwords.
h. Do not write down passwords or store passwords online.
i. Do not talk about any passwords in front of others.
j. Do not share your format for constructing a password (e.g., "my family name")
k. Do not reveal a password on questionnaires or security forms.
l. Do not share a password with family members.
m. Do not reveal a password to co-workers while on vacation.
n. Do not use the "Remember Password" feature of applications (e.g. Outlook, web browsers, etc.) that remember your password when the username is entered.

o. Do not store passwords in a file on ANY computer system including mobile devices without encryption.
p. Passwords should be changed at least once every six months.

Passwords are considered "strong" passwords when they contain the following:

a. Both upper and lower case characters (e.g., a-z, A-Z)
b. A combination of digits, punctuations, and letters e.g., 0-9,!@#$%^&*()_+|~- =\`{}[]:";'<>?,./)
c. At least eight alphanumeric characters long

Note: There is no uniformity as to which special characters are allowed to be used in passwords. Users will be informed of specific system password characteristics requirements including any excluded characters. It is recommended that all passwords be based on strong password construction criteria to that extent allowed by each system even if enforcement is not in place.

Password Reset Frequency

Athens State University account passwords will be configured to force a change on a 120-day cycle.

III. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the President has assigned the Provost/Vice President for Academic Affairs as the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every two years or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer.

Policy Number: VI.03
Policy Level: Operating Policy
Originally Issued: December 4, 2013
Revised: April 13, 2016
Reviewed: May 15, 2018
Reviewed: June 8, 2020
Reviewed: November 3, 2022
Policy Owner: Provost/VP for Academic Affairs
Policy Implementation: Chief Information Officer
SACSCOC Standard: 10.6