Name of Policy	Password Policy
Description of Policy	The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
Policy applies to	☒ University-wide ☐ Specific
	☐ Staff only ☐ Students only ☒ Staff and students
Policy status	☐ New policy ☒ Revision of existing policy

Approval authority	Center for Information Technology Services
Governing authority	Finance and Administrative Services
Responsible officer	Chief Information Officer

Approval date	
Effective date	November 1, 2022
Approval date of last revision	December 01, 2017
Effective date of last revision	December 01, 2017
Date of policy review*	November 1, 2025

**unless otherwise indicated, this policy will still apply beyond the review date*

Related legislation, policies, procedures, guidelines and local protocols	

Suggested headings for Table of Contents

1. Background

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of Alcorn's State University's entire network. As such, all Alcorn State University students, and employees (including contractors and vendors with access to Alcorn State University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

This policy describes the University's requirements for acceptable password selection and maintenance. It provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password. Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Passwords must, therefore, follow the policy guidelines listed below.

3. Scope/Application

This policy applies to anyone accessing systems that hold or transmit Alcorn State University data. Systems include, but are not limited to personal computers, laptops, Alcorn State University issued cell phones, and small factor computing devices (e.g., tablets, USB memory keys, electronic organizers), as well as Alcorn State electronic services, systems, and servers. This policy covers departmental resources as well as resources managed centrally.

4. Policy Statement and Principles

All passwords shall be constructed and implemented according to the following criteria:

- Passwords must be treated as confidential information.
- Passwords shall be routinely changed every 1 year or less.
- Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups; stored procedures) are not subject to the routine change specified here. Service account passwords must be changed with changes in personnel (termination, change in duties, transfer, etc.).
- Owners of systems that maintain mission critical and/or confidential information shall establish a reasonable period for passwords to be maintained in history to prevent their reuse.
- Passwords should not be anything that can be easily associated with the account owner such as: username, social security number, UIN, nickname, relative's name, birth date, telephone number, etc.
- Passwords should not be dictionary words or acronyms regardless of language of origin and must be unique.
- Stored passwords shall be encrypted.
- Passwords shall never be transmitted as plain text.
- There shall be no more than seven tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial- and-error" attacks on passwords.

- Security tokens (e.g., Smartcard) must be returned when there has been a change in job duties which no longer require restricted access, or upon termination of employment.
- If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s).
- Users shall not circumvent password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always enter "no" when asked to have a password "remembered".
- Exceptions may be made for specific applications (like automated backup) with the approval of the information resource owner. For an exception to be approved, there must be a procedure for the user to change passwords.Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.
- Forgotten passwords shall be replaced, not reissued.
- Procedures for setting and changing information resource passwords include the following:
- The user must verify his/her identity before the password is changed.
- The password must be changed to a "strong" password – (see section 5 of password guidelines below); and,
- The user must change password at first log on – where applicable.
- Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service.
- Automated password generation programs must use non-predictable methods of generation, should be unique; and,
- Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.
- Password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as:
- Time and date of password change, expiration, administrative reset.
- Type of action performed; and,
- Source system (e.g., IP and/or MAC address) that originated the change request.

All servers and workstations shall have passwords that conform to this Policy.

PASSWORD GUIDELINES TO CREATE STRONG PASSWORDS

Make the password difficult to guess, but easy to remember.

- Passwords should contain at least three of the following:
  1. Upper case characters (A-Z).
  2. Lower case characters (a-z).
  3. A special character – as permitted by computing systems (such as: !#$%^*<>); and,
  4. Numeric characters.
  5. Be at least 12 characters long.

Avoid passwords that are known to be stolen or compromised.

When possible, use multi-factor authentication, such as Azure MFA

Passwords should not be easily guessed or "weak." Do not choose passwords that are:

1. Your username.
2. Names of family, pets, friends, co-workers, etc.
3. Words associated with your school, school mascot, etc. (such as, "ASU or Alcorn" and "panther"

4. Other personal information easily obtained such as: birthdays, addresses, phone numbers, and license plate numbers.
5. Word or number patterns (e.g., aaabbb, qwerty, 123321).

Any of the above spelled backwards.

1. Any of the above preceded or followed by a digit (e.g., secret1, 1secret); and,
2. Certain devices (such as voice mail access from a telephone) require password entry through numeric keypad. In this case, users shall avoid using telephone numbers in any format (5 digit such as 5-3211, 7 digit such as 845-3211 or 10 digit such as 979-845-3211) as the password.

5. Roles and Responsibilities

Violations of this policy may result in loss of Alcorn State University system and network usage privileges, disciplinary action, up to and including termination or expulsion as outlined in applicable Alcorn State University Employment policies and the Alcorn State University Student Code of Conduct.

6. Revision made to this Policy

- Increase maximum password age from 90 days to 365 days
- Increase minimum password length from 8 to 12 characters
- Increase participation scope to include all users accessing systems that hold or transmit Alcorn State University data.
- Additional information added to Policy Statement and Principles

7. Further Assistance

Contact the Help Desk at: (601) 877-6182 (You will be asked to provide information to verify your identity).

8. Glossary of Terms/Definitions*

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements.

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Mission Critical Information - information that is defined by the university or information resource owner to be essential to the continued performance of the mission of the university or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the university or department.

Information Security Officer (ISO) – person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

REVIEWED BY:

/s/ Cornelius Wooten, Ph.D. October 13, 2022

Senior Vice President for Finance, Administrative Services and Operations/CFO — Date

/s/ Alfred L. Galtney, J.D. October 13, 2022

Chief Compliance Officer — Date

APPROVED:

/s/ Felecia M. Nave, Ph.D. October 13, 2022

President/IEO — Date