FAYETTEVILLE STATE UNIVERSITY

PASSWORD, PASSPHRASE, AND AUTHENTICATION CONTROLS

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Board of Trustees.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff ●Students
History:	Revised – January 18, 2024 First Issued – August 4, 2023
Related Policies/ Regulations/Statutes:	●Information Security
Contact for Info:	Vice Chancellor for Information Technology and Chief Information Office (910) 672-1477

I. PURPOSE

The purpose of this policy (Policy) is to ensure that all Fayetteville State University (University) information systems and applications protect the confidentiality, integrity, and availability of information resources accessed, managed, and/or controlled by the University.

In accordance with the University's *Information Security Related to University Personnel* policy and in support of its *Information Systems Access Control* policy, this Policy sets forth password/passphrase requirements for all University individual user accounts, administrator accounts, and system accounts. All authentication methods used to access computing systems that connect to the University network or contain University data must meet the specific minimum requirements described below and must be traceable to individual users. Any suspected compromise of a passphrase must be reported immediately in compliance with the University's *Incident Management* policy.

This Policy sets minimum requirements. group, unit, or departmental policies, or specific system security requirements may impose more stringent or additional requirements than the minimum set forth here. Best practice guidance may also exceed these minimum requirements.

NOTE: These requirements must be met even if a system does not enforce the requirements with technical controls (users must select passphrases meeting or exceeding these policies even when a system would allow a weaker passphrase).

II. DEFINITIONS

The following definitions are used in this Policy:

- **Administrator:** User account with higher privileges than a standard user of an application or operating system. This includes administrators of servers, multi-user applications, privileged access to applications, or sudo access. A user who can set privilege levels for other users is an administrator. NOTE: This does not include common use of "local admin" privileges on individual devices.
- **sensitive:** Access privileges granted to a user, program, or process or the act of granting those privileges.
- **Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Facial recognition:** The use of camera(s) to uniquely identify an individual.
- **Fingerprint:** The use of a fingerprint reader to uniquely identify an individual.
- **Password/Passphrase:** A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.
- **PIN:** A typically numeric code used to authenticate to a hardware component.
- **Public key cryptography:** Cryptography using the NIST-approved algorithms when the private key is safeguarded (e.g., password protected, physically safeguarded, etc.)
- **Sensitive Information:** Information classified as Confidential or Internal Use Only in the University’s *Information Classification* policy.

III. AUTHENTICATION METHODS

Users are encouraged to use authentication methods that exceed the minimum requirements where available. Examples include stronger passphrases, facial recognition, fingerprint-scans, public key cryptography, etc.

Departments may employ additional or more stringent requirements but may not permit authentication methods less stringent than those described in this Policy.

A. <u>Passphrase Requirements</u>

All University individual users, administrators, and system accounts are required to use a password/passphrase and/or other authentication method(s) in accordance with this Policy.

All passphrases used to access computing devices that connect to university resources must meet the specific minimum requirements described in this Policy and must be traceable to individual users. Any suspected compromise of a passphrase must be reported in accordance with the University *Incident Management Procedure*.

The following are system account passphrase requirements for users, and administrators:

- Systems and applications may use additional mechanisms to protect accounts (such as forbidding either re-use of a passphrase or passphrases that are too simple).
- Passwords granting access to university information resources must minimally meet these requirements:
    - Passwords must be at least fifteen (15) characters in length
    - Passwords must contain at least three (3) of these four types of characters:
    - Upper-case alpha characters [A-Z]
    - Lower-case alpha characters [a-z]
    - Numeric characters [0-9]
    - Special characters [! @#$%^&*()_+|~-=\`{}[]:";'<>?,./]
- Passwords must be changed in accordance with the requirements below:
    - All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed at least once per year.
    - All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every year.
    - Any password that is suspected of having been compromised must be changed immediately.
    - User accounts must have unique passwords; the same password must not be used for multiple user accounts.
    - When passwords are changed, users must not use any of the previous twenty-four (24) passwords used for that user account.
- Use of 2-factor or multi-factor authentication is required wherever it is available.
- The same passphrase should not be used on both University systems and non-University systems. A unique passphrase for each system is strongly recommended. Default passwords must be changed and are not permitted.
- All passphrases should be treated as restricted sensitive information. Passphrases should not be shared with others, except in emergency situations (see "System Accounts" and "Exceptions" below for special cases). Users may only use account credentials for which users have been authorized. Users are responsible for maintaining the security of their passphrases.

B. Authentication Configuration Requirements

System and application administrators or others who are responsible for managing or contracting for a system or application that requires authentication, must ensure that at a minimum it meets one of the following configuration options:

1. Option 1: The University issued user ID shall be used if it is technically and operationally feasible.

    - System or application uses the University issued user ID to provide authentication services. (Azure AD)
    - Where feasible requires 2-step or multi-factor authentication.

OR

2. Option 2:

    - Require a minimum of 14 characters of any type and allow longer passphrases.
    - Requires new passphrases to be substantially different from previous passphrases.
    - Where technically feasible, requires 2-step or multi-factor authentication for any accounts allowed access to Tier 2 or Tier 3 data other than self-service for the account owner.
    - Prohibits repetition of characters/words/sequences.
    - Prohibits the use of passphrases which have been exposed in breaches on that system.
    - Requires passphrase changes at least every year.

OR

3. Option 3, Legacy systems (Only to be used for systems which cannot be configured for Option 1 or 2):

    - Require a minimum of 8 characters.
    - Contain at least one upper-case letter, at least one lower-case letter and at least one numerical digit.
    - Contain at least one of these characters: !@#$%&*+={}?<>"'.
    - Not start with a hyphen, end with a backslash (\), or contain a double quote (") anywhere except as the last character.
    - Require passphrase changes at least every 90 days.
    - Require new passphrases to be substantially different from previous passphrases if technically feasible.

- Require use of 2-step or multi-factor authentication for any accounts allowed access to Tier 2 or Tier 3 data other than self-service for the account owner.
- Consultation with ITS Information Security Office is required to document technical infeasibility and risk analysis should 2-step or multi-factor authentication be unavailable for accounts accessing Tier 2 or Tier 3 data other than self-service for the account owner.

University units may employ more stringent authentication requirements or additional authentication methods, such as public key cryptography (must be revoked when key has been compromised), beyond those outlined in this document but may not allow less stringent authentication than listed here unless an exception applies.

C. Exceptions

Compliance with previous Password Policy/Policy documents superseded by this Policy are sufficient until password reset as previously scheduled. At that time, compliance with this Policy is required.

D. Specialty Devices

Due to the wide variety of specialty devices and their frequently limited capabilities, particularly with regard to passphrase management, specialty devices (e.g., fax machines, printers, physical access control equipment, copy machines, specialty lab equipment, phones) are not subject to this Policy *unless* those devices are used to store or protect sensitive information *or* perform mission-critical functions *or* are able to be configured with a unique login ID and/or password. Where appropriate, departments should develop their own specific rules for the specialized devices to ensure that adequate authentication controls are present.

E. Service Accounts

Service accounts (also known as System or Device accounts) are typically not associated with an individual user. These accounts are used to run IT services for applications (e.g., Web services, database services, an application account created to run a specific application) or as built-in accounts in an operating system or application (e.g., “root” or “system” or “admin”). Service accounts must only be used for system services. Use of a standard user account to run system services is prohibited, and exceptions do not apply to standard user accounts. Individuals must not log in using service account credentials except as needed in the scope of supporting the specific service/system. Systems should be configured to prevent remote logins to service accounts wherever technically feasible. Default passwords must be changed and are not permitted. Requirements not listed below as exceptions are in force (17 character minimum, for example). With those constraints in place, in order to ensure that key services are not disrupted, and because some requirements of this Policy may be technically infeasible for service accounts, some exceptions apply:

These accounts may be managed by more than one individual (an exception to the passphrase-sharing prohibition). Passphrases must be changed when an individual with access to the passphrase leaves the department and the individual may still be able to login.

- No lock-out period is required.
- Log-in renewal is not required.
- Multi-factor authentication is not required
- Accounts may use public key cryptography (revoked when key has been compromised) rather than passphrases
- Device-specific authorization may substitute for other authentication methods

Use of login/usage review as a compensating control is strongly recommended for service accounts.

F. <u>Single-device authentication</u>

Passphrases are not required to access a device where a single-device authentication mechanism such as a hardware+PIN, fingerprint-scan, or facial recognition is in use. Such devices have a hardware module that deters brute-force attacks and require physical access to the device, as such, other length and complexity requirements are not required, and these mechanisms may substitute for use of a passphrase.

Devices that support Microsoft Windows Hello for Business exceed the minimum requirements of this Policy and are an acceptable alternative. For use of hardware+PIN, hardware components must inhibit brute force attacks and PINs must be at least 6 characters in length.

Departments wishing to allow the use of proximity cards/tokens may do so if documented best practices are in place (e.g., token cannot be left near computer, report lost/stolen tokens, etc.).

V. EXCEPTIONS

Exceptions to this Policy may be made by the Vice Chancellor for Information Technology and Chief Information Officer (CIO) or their delegate(s). Approval of such exceptions must be in writing. Exceptions may also be defined in other related or supporting policies.

VI. EXTERNAL REGULATIONS AND CONSEQUENCES

Failure to comply with this Policy may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this Policy may be referred to the appropriate University student conduct office(s). Contractors, vendors, and others who fail to adhere to this Policy may face termination of their business relationships with the University.

Violation of this Policy may also carry the risk of civil or criminal penalties.