FAYETTEVILLE STATE UNIVERSITY

INFORMATION SYSTEMS ACCESS CONTROL

Authority: Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor es may only be made by the Board of Trustees.

Category: Information Technology

Applies to: ●Administrators ●Faculty ●Staff ●Students

History: **I**ssued – October

Related Policies/ Regulations/Statutes: ●*Information Security* ●*End User Information Security*

Contact for Info: Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

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

II. DEFINITIONS

The following definitions are used in this Policy:

- **Access** shall mean the ability to view, use, or change information in University information resources.

- **Availability** shall mean degree to which information and critical University services are accessible for use when required.

- **Confidentiality** shall mean degree to which confidential University information is protected from unauthorized disclosure.

- **Information Owner** shall mean an **i**ndividual with primary responsibility for overseeing the collection, storage, use, and security of a particular information resource. In cases where an Information Owner is not identified for any information resource, the cognizant Vice Chancellor or Dean shall be deemed the Information Owner.

- **Information Resource** shall mean Data, information, and information systems used by University to conduct University operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

- **Information Security** shall mean **t**he protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

- **Integrity** shall mean The degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

- **Principle of Least Privilege** shall mean that a user account or process will be granted to only those privileges which are essential to perform its intended function.

- **Privileged Access** shall mean access that allows the grantee non-standard or elevated permissions allowing access to administrate systems or data. This includes the ability to modify system configurations, manage software systems, grant access, etc. It also includes elevated access to the University's data enabling direct data management, data maintenance, or reporting. Privileged access may also be referred to as "administrator" or "admin" access.

- **Privileged Use** shall mean any individual granted privileged access to information, systems, or databases that extends beyond access to one's own self-service data.

III. BUSINESS REQUIREMENT FOR ACCESS CONTROL

Each University system and application should have a clearly defined and documented policy statement defining the access rights of each user (or group of users). These policies should be established based on business requirements, approved through a formal and auditable process, and regularly reviewed.

IV. USER ACCESS MANAGEMENT

University systems and applications must meet the following requirements governing the management of access to information resources:

- A formal registration and de-registration procedure for granting and revoking access will be defined and documented.
- The assignment and use of rights and privileges will be restricted and controlled.
- Access to all systems will be authorized by the system owner and a record maintained of the authorization and access rights or privileges assigned.
- Procedures will be established to ensure user access rights are modified appropriately based on changes in business need, role, or status.
- Access will be granted following the Principle of Least Privilege. By default, access will be denied to information resources and opened only to individuals when access is required to perform an assigned job duty. Where access is needed, only the minimum access level required to accomplish the work responsibility will be granted.
- Passwords will be controlled through a formal management process.
- User access rights will be reviewed by Information Owners at regular intervals using a formal process.

V. USER ACCOUNTS

University employees and students must use unique user accounts (logon IDs) when accessing

University information resources. These user accounts must uniquely identify the individual and the individual is responsible for the use and misuse of their assigned user accounts.

University user account names should not be associated with non-University systems. Thus, a University email address should not be used as a username for a logon account for a personal website (online banking, travel, social media, etc.)

University systems will enforce the deactivation or lockout of user accounts after a maximum of five unsuccessful login attempts. Once the account is locked or disabled, it will remain locked for one hour (60 minutes). After one hour, the user account will unlock and become usable again.

VI. PASSWORDS

Passwords are critically important to the overall security of University information resources. A poorly chosen or improperly protected password may result in the compromise of the University's systems or networks. As such, all University employees and students are responsible for selecting an appropriate password based on the information provided below and securing that password.

Passwords granting access to University information resources must minimally meet these requirements:

- Passwords must be at least twelve (12) 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 90 days.
- 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 five (5) passwords used for that user account.

Users should adhere to the following to protect their account passwords:

- All passwords must be treated as confidential University information; thus, passwords should not be shared.
- Long passwords should be used.
- The following should not be used as passwords:
  - Words that refer to personal data (i.e., children's names or your birth date).
  - Dictionary words.
  - Short words.
- Passwords should not be revealed on questionnaires or security forms.
- The "Remember Password" feature in Windows or applications (e.g., Internet Explorer, Outlook, Firefox, Google Chrome, etc.) should not be used.

- Passwords should not be written down and stored where accessible by others.
- Passwords should not be input while individuals are watching.
- Contact the Information Security Office / Officer (ISO) if an individual demands a password.

In addition to the ability to support the requirements detailed above, the University developed, or deployed systems will also support the following password requirements:

- Systems will support the identification and authentication of individual users (not just groups).
- Systems will not store passwords in clear text or in any form that is reversible back to the original password.
- Stored passwords will be salted and hashed using a cryptographically strong, one-way hash function.
- Passwords will be masked or suppressed on all application screens.
- Passwords will not be included in any system or application log files.

VII. MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor authentication strengthens the University's security posture by lowering the risk that compromised credentials can be used to provide unauthorized access to the University's systems and data. Multi-factor authentication must be used in the following scenarios:

- Remote logins to University internal network (VPN)
- Logins to any systems or applications that are accessible remotely via the Internet (Citrix, web applications, system logins, etc.)
- Privileged access login to University systems and applications.
- Logins to the University email system

Logins to other systems and applications should utilize multi-factor authentication wherever possible and feasible.

VIII. PRIVILEGED ACCESS

Privileged access enables an individual to take actions which may affect the University's information resources or the accounts or processes of other users. Privileged access is typically granted to system, network, and application administrators whose job duties require special privileges to support the operations of a system, network, or application.

In addition to requirements included in this Policy, systems and applications must meet the following requirements governing the management of privileged access to information resources:

- Privileged access will only be granted to authorized individuals.
- Privileged access will be assigned to a dedicated account for performing privileged administrative duties.
- Privileged access may only be used when performing administrative job duties that require elevated permissions.
- Administrative credentials are not to be used as a primary login for non-privileged access and activities, such as web browsing or reading email.
- Privileged access will not be used for unauthorized viewing, modification, copying, or destruction of system or user data.

- Privileged access will be granted following the Principle of Least Privilege.
- Systems will be configured to log all privileged access with an accurate timestamp.
- Privileged users must respect the privacy and rights of system users.
- Privileged users must respect the integrity of University systems and data.
- Privileged users must protect the confidentiality of any information they encounter while performing their duties.
- Privileged users must comply with all applicable University policies and procedures as well as local, state, and federal law and regulations.

IX. ATTESTATION AND ENTITLEMENT REVIEWS

Information Owners should review users' access privileges at regular intervals. The review of access privileges should consider the following:

- Users' access privileges should be reviewed at regular intervals (at least annually) and after any changes in University status, job, or role.
- Privileged access should be reviewed at least quarterly and after any changes in University status, job, or role.
- Privileged access should be audited at regular intervals to ensure unauthorized privileges have not been granted.
- Information Owners must maintain documentation that demonstrates access review was performed, and this documentation must be available for review as required.

X. TERMINATION OF ACCESS

When an individual's association with the University ends (whether voluntary or involuntary), the IT Services Help Desk or ISO must be promptly notified of the change. If the association is ending voluntarily and the individual provides advance notice, the individual's University contact (e.g., supervisor, unit head) must promptly notify the IT Services Help Desk of the individual's last scheduled day of work so their access can be revoked appropriately. The individual's University contact is responsible for ensuring all keys, ID badges, other access devices, computing equipment, and other property is returned to the University prior to the individual leaving on their final day.