ELIZABETH CITY STATE UNIVERSITY
Information Systems Access Control Policy

1. PURPOSE

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

2. SCOPE

This policy applies to all ECSU employees and students, whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the ECSU community.

3. ACRONYMS / DEFINITIONS

Access. The ability to view, use, or change information in ECSU information resources.

Availability. The measures to which information and critical ECSU services are accessible for use when required.

Confidentiality. The measures to which confidential ECSU information is protected from unauthorized disclosure.

Information Owner. An Information Owner has 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 President or Dean shall be deemed the Information Owner.

Information Resource. Data, information, and information systems used by ECSU to conduct ECSU 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. The 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. The measures to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the ECSU.

Principle of Least Privilege. This principle states a user account or process will be granted only those privileges which are essential to perform its intended function.

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

Privileged User. Any individual granted privileged access to information, systems, or databases that extends beyond access to one's own self-service data.

4. POLICY

A. BUSINESS REQUIREMENT FOR ACCESS CONTROL

Each ECSU 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.

B. USER ACCESS MANAGEMENT

ECSU systems and applications will meet the following requirements governing the management of access to information resources:

i. A formal registration and de-registration procedure for granting and revoking access will be defined and documented.
ii. The assignment and use of rights and privileges will be restricted and controlled.
    a. Access to all systems will be authorized by the system owner and a record maintained of the authorization and access rights or privileges assigned.
    b. Procedures will be established to ensure user access rights are modified appropriately based on changes in business need, role, or status.
    c. 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.
iii. Passwords will be controlled through a formal management process.
iv. User access rights will be reviewed by Information Owners at regular intervals using a formal process.

C. USER ACCOUNTS

ECSU faculty, staff, and students will use unique user accounts (logon IDs) when accessing ECSU 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.

ECSU user account names will not be associated with non-ECSU systems. As an example, do not use your ECSU email address as a username for a logon account for a personal website (online banking, travel, social media, etc.)

ECSU 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.

D. PASSWORDS

Passwords are critically important to the overall security of ECSU information resources. A poorly chosen or improperly protected password may result in the compromise of ECSU systems or networks. As such, all ECSU faculty, staff, and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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

i. Passwords must be at least twelve (12) characters in length
ii. Passwords must contain at least three (3) of these four types of characters:
    a. Upper-case alpha characters [A-Z]
    b. Lower-case alpha characters [a-z]
    c. Numeric characters [0-9]
    d. Special characters [!@#$%^&*()_+|~-=\` {}[]:";'<>?,./]
iii. All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed at least once per year.
iv. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every 90 days.
v. Any password that is suspected of having been compromised must be changed immediately.
vi. User accounts must have unique passwords, the same password must not be used for multiple user accounts.
vii. When passwords are changed, users must not use any of the previous five (5) passwords used for that user account.

To protect user account passwords, these practices are recommended:

i. Never share your password with another individual, including administrative assistants, graduate assistants, IT Services staff, co-workers, family, friends, etc. All passwords must be treated as confidential ECSU information.
ii. Use longer passwords. Longer passwords are stronger passwords.
iii. Do not use passwords that refer to personal data (e.g., children's names or your birth date).
iv. Do not use passwords that contain dictionary words.
v. Do not reveal a password on questionnaires or security forms.
vi. Do not use the "Remember Password" feature in Windows or applications (e.g. Internet Explorer, Outlook, Firefox, Google Chrome, etc.).
vii. Do not write passwords down and store them anywhere accessible by others.
viii. Do not type your password when someone is looking over your shoulder.
ix. If someone demands a password, refer them to this document and then contact the Information Security Officer (ISO).

In addition to the ability to support the requirements detailed above, systems developed or deployed by ECSU must also support the following password requirements:

i. Systems must support the identification and authentication of individual users (not just groups).
ii. Systems must not store passwords in clear text or in any form that is reversible back to the original password.
iii. Stored passwords must be salted and hashed using a cryptographically strong, one-way hash function.
iv. Passwords must be masked or suppressed on all application screens.
v. Passwords must never be included in any system or application log files

E. MULTI-FACTOR AUTHENTICATION (MFA)

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

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

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

F. PRIVILEGED ACCESS

Privileged access enables an individual to take actions which may affect ECSU 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 defined within Section 4.B, ECSU systems and applications must meet the following requirements governing the management of privileged access to information resources:

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

vii. Systems will be configured to log all privileged access with an accurate timestamp.
viii. Privileged users must respect the privacy and rights of system users.
ix. Privileged users must respect the integrity of ECSU systems and data.
x. Privileged users must protect the confidentiality of any information they encounter while performing their duties.
xi. Privileged users must comply with all applicable ECSU policies and procedures as well as local, state, and federal law and regulations.

G. ATTESTATION AND ENTITLEMENT REVIEWS

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

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

H. TERMINATION OF ACCESS

When an individual's association with ECSU 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 ECSU contact (e.g. supervisor, Department Head, etc.) must promptly notify the IT Services Help Desk of the individual's last scheduled day so their access can be revoked appropriately. The individual's manager is responsible for ensuring all keys, ID badges, other access devices, computing equipment, and other property is returned to ECSU prior to the individual leaving on their final day.

5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate to the severity and/or frequency of offense and can include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.