# ELIZABETH CITY STATE UNIVERSITY
# Information Classification and Handling Policy

## 1. PURPOSE

The purpose of this policy is to establish requirements for ensuring the security and confidentiality of sensitive information within the Elizabeth City State University (ECSU) community, and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information. This policy outlines essential roles and responsibilities for creating and maintaining an environment that safeguards data from threats to personal, professional, and institutional interests, and establishes a comprehensive data security program in compliance with applicable law.

## 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. This policy applies to all information collected, stored, or used by or on behalf of any operational unit, department and person within the community in connection with ECSU operations. In the event that any particular information at ECSU is governed by more specific requirements under other ECSU policies or procedures, the more specific requirements shall take precedence over this policy to the extent there is any conflict.

## 3. ACRONYMS / DEFINITIONS

***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.

***Control.*** Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

***Control Statement.*** Statements provided in addition to classification labeling to further restrict or clarify how the information is to be handled, for example, “To be Opened by Addressee Only” or “Classified Public after 01/01/2020”.

***Family Educational Rights and Privacy Act (FERPA).*** The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the

U.S. Department of Education. For more information regarding FERPA, visit the U.S. Department of Education at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

***General Data Protection Regulation (GDPR).*** The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. For more information regarding GDPR, visit EU GDPR.org at https://eugdpr.org/

***Gramm-Leach-Bliley Act (GLBA).*** The Gramm Leach Bliley Act (GLBA) is a law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. For more information regarding GLBA, visit EDUCAUSE at https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act.

***Health Insurance Portability and Accountability Act (HIPAA).*** The Health Insurance Portability and Accountability Act of 1996 was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. For more information regarding HIPAA, visit the U.S. Department of Health & Human Services at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

***Information Resource.*** Data, information, and information systems used by ECSU to conduct business 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 ECSU.

***The Division of Information Technology (DIT).*** The Division of Information Technology staff have primary operational responsibility for information systems that receive, create, store, handle, or discard information.

***Payment Card Industry (PCI).*** Credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

A. Cardholder name
B. Service code
C. Expiration date
D. CVC2, CVV2 or CID value
E. PIN or PIN block
F. Contents of a credit card's magnetic stripe

***Personally Identifiable Information (PII).*** Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

***Protected Health Information (PHI).*** Any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

***Security Breach or Security Compromise.*** An unauthorized intrusion into an ECSU information resource where unauthorized disclosure, modification, or destruction of sensitive or confidential information may have occurred.

***Security Event.*** A system, service, or network state, condition, or occurrence indicating information security may have been breached or compromised or that an information security policy may have been violated or control may have failed.

***Security Incident.*** An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

***Vulnerability.*** A weakness in ECSU's operating environment that could potentially be exploited by one or more threats.

## 4. POLICY

ECSU community has a responsibility to protect the confidentiality, integrity, and availability of ECSU information collected, processed, stored, or transmitted regardless of the location or medium on which the information resides. Information must be classified and handled according to its value, legal requirements, sensitivity, and criticality to ECSU. Safeguards must be established and implemented relative to the information's classification, protecting information from unauthorized access, modification, disclosure, and destruction.

## A. CLASSIFICATION OF INFORMATION

All ECSU information collected, processed, stored, or transmitted by any means shall be classified into one of four categories, according to the level of sensitivity (in descending order): *Sensitive, Confidential*, *Internal Use Only*, and *Public*. Sensitivity defines information in terms of what the data is and how access to, processing, communication, and storage of this data must be controlled and secured.

All information resources, whether physical documents, electronic databases, electronic files, or other collections of information, are to be assigned an information classification level according to the most sensitive content contained therein. If more than one information classification level applies, the highest level (most restrictive) should be selected.

### i. SENSITIVE

*Sensitive* information is information whose unauthorized access, use, modification, disclosure, or destruction would cause significant embarrassment or damage to the operations, finances, and reputation of ECSU or to affected faculty, staff, and/or students. Exposure of certain *Sensitive* information will require ECSU to report such exposure to various Federal and State agencies and/or financial institutions as well as to the individuals whose information was exposed.

Examples of *Sensitive* information include but not limited to:

a. Personally Identifiable Information (PII)
b. Social Security number
c. Driver's license number
d. Passport and visa numbers
e. Unlisted telephone numbers, student directory information requested not be disclosed
f. Personal financial information, including bank / credit / debit card numbers
g. Federal individual financial aid / grant information
h. Protected Health Information (PHI) and medical records
i. Employee personnel file / disciplinary information
j. Human Resources information of individual applicants
k. Admission applications
l. Individual student counseling / disciplinary information
m. Individual student grades / records
n. Privileged data in the Office of the General Counsel
o. Criminal complaints and investigations, police records, and evidentiary materials
p. Information security data, including passwords and sensitive information related to ECSU's information technology infrastructure and operations.
q. Information not available to the public under all privacy laws, including but not limited to:
    1. Family Educational Right to Privacy Act (FERPA)

2. General Data Protection Regulation (GDPR)
3. Gramm-Leach-Bliley Act (GLBA)
4. Health Insurance Portability and Accountability Act (HIPAA).

**ii. CONFIDENTIAL**

*Confidential* information is information whose unauthorized access, use, modification, disclosure, or destruction could adversely impact operations, finances, and reputation of ECSU or to affected Third-Party suppliers, faculty, staff, and/or students. Exposure of certain *Confidential* information may require ECSU to report such exposure to various Federal and State agencies and/or financial institutions as well as to the individuals whose information was exposed.

Examples of *Confidential* information include but not limited to:

a. Education records such as grades and class schedules
b. The University's proprietary information including, but not limited to, intellectual research findings, intellectual property, financial data, and donor/funding sources
c. Confidential personnel file information protected by the N.C. Human Resources Act, including criminal background check results
d. Attorney-client communications
e. Information subject to a confidentiality agreement
f. Information protected by contractual agreements or non-disclosure agreements such as vendor product roadmaps, bid documents sealed for a limited time

**iii. INTERNAL USE ONLY**

*Internal Use Only* information is information less sensitive than *Confidential* information, but that, if exposed to unauthorized parties, may cause embarrassment or damage to the operations, finances, and reputation of ECSU or to effected faculty, staff, and/or students.

Examples of *Internal Use Only* information include, but is not limited to:

a. Internal memos meant for limited circulation that do not include *Confidential* information
b. Internal ECSU policies and operating procedures that do not include *Confidential* information
c. Draft documents subject to internal comment prior to public release
d. Employee place of birth, home address, evaluations, resumes
e. Individual employee salary and benefit data
f. Vendor contracts
g. Invoices and internal billing
h. Detailed annual budget information
i. Financial transactions that do not include *Confidential* data

**iv. PUBLIC**

*Public* information is information that is generally available to the public, or if made public, would have no material adverse effect on the operations, finances, and reputation of ECSU or faculty, staff, and students.

Examples of Public information include, but not limited to:

a. Press releases, marketing materials, ECSU brochures, ECSU calendars
b. Articles, White Papers, etc. written for external review
c. Faculty/staff bios
d. Course catalogs
e. Email sent for ECSU distribution

## B. ROLES AND RESPONSIBILITIES

All members of the ECSU community share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigns specific duties to specific roles within ECSU. It is likely that an individual will have responsibilities reflecting multiple roles with respect to certain information.

**i. Information Security Officer (ISO)**

The Information Security Officer has authority and responsibility for the operation and management of ECSU's Information Security Program. The ISO is required to perform or delegate the following information security responsibilities:

a. Establish, document, and distribute information security polices, standards, procedures, and guidelines.
b. Develop and implement a risk assessment process to identify, analyze, and mitigate risks to ECSU information resources.
c. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of violation, breach, or compromise.
d. Implement practical and effective technologies and services to ensure the security of ECSU information resources, networks, and computing infrastructure.
e. Disconnect any device or disable any account believed to be involved in compromising security of ECSU information resources until the device or account no longer poses a threat.
f. Develop and implement an information security awareness program to be offered periodically to all ECSU faculty, staff, and students.

**ii. Division of Information Technology (DIT)**

Division of Information Technology staff have primary operational responsibility for information systems that receive, create, store, handle, or discard information. DIT shall be responsible for:

a. Implementing information security technologies, controls, and services to protect information resources as required by the Information Security Program.

b. Granting and revoking user rights to information resources and privileged user access to information systems as directed by the ISO or information resource owners.
c. Ensuring availability and recovery of information resources.
d. Abiding by the requirements of the Information Security Program.

**iii. Vice Chancellors and Deans**

Vice Chancellors and Deans (including the ECSU Chancellor and other members of the senior leadership team) shall be responsible for protecting all ECSU information resources within their respective offices or departments by:

a. Managing the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
b. Determining the proper levels of protection, through consultation/coordination with the ISO, for office or department information resources and ensuring necessary safeguards are implemented.
c. Protecting information resources used by the office or department are assigned an Information Owner.
d. Promoting information security awareness in the office or department and ensuring all staff participate in relevant university-provided security and privacy training.
e. Requiring staff to complete FERPA and HIPAA training provided by Human Resources, and Information Security Training provided by the Division of Information Technology.
f. Authorizing end user access to information resources appropriate for the user's job function.
g. Requiring staff to acknowledge their responsibilities for compliance with Information Security Policies.

**iv. Information Owners**

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

An Information Owner is responsible for:

a. Ensuring information resources are assigned a security classification and labeling (including control statements) where appropriate.
b. Clearly identifying *Sensitive, Confidential* and *Internal Use Only* information when sharing or providing individuals, departments, or third parties with access.
c. Establishing security requirements and expectations for information resources within their ownership:
    1. Information User authentication
    2. Information User access lifecycle management (request, approve, provision, review, and revoke)
    3. Record retention

d. Providing training and awareness specific to information protection and handling of their *Sensitive, Confidential* and *Internal Use Only* information.
e. Maintaining an inventory of their information resources, including all applications that collect, process, store, or transmit their information.
f. Conducting periodic entitlement and attestation reviews of access granted to *Sensitive, Confidential* and *Internal Use Only* information.
g. Reviewing, at least annually, information classification based on changes in value, legal requirements, sensitivity, or criticality to ECSU and updating as appropriate.
h. Establishing procedures for data destruction.
i. Performing risk assessments, at least annually, of information resources to review requirements as needed to address changing risks, ECSU requirements, or laws and regulations.
j. Ensuring compliance with regulatory requirements such as FERPA, GDPR, GLBA, HIPAA, PCI, and other State, Federal, and contractual requirements that may apply.

**v. Information Users**

Information Users shall be responsible for:

a. Reviewing, understanding, and complying with all relevant ECSU information security policies, standards, procedures, and guidelines.
b. Providing appropriate physical security for information technology equipment, storage media, and physical data.
c. Ensuring sensitive or confidential information is not distributed or accessible to unauthorized persons.
d. Protecting the confidentiality of personal passwords, never sharing under any circumstance.
e. Logging off from all applications, computers, and networks, and physically securing printed material, when not in use.
f. Immediately notifying the DIT Help Desk and the ISO of any incident that may cause a security breach or violation of information security policy.
g. Abiding by the requirements of the Information Security Program.

**vi. CHIEF HUMAN RESOURCE OFFICER (CHRO)**

The CHRO shall be responsible for:

a. Collaborating with the ISO to educate incoming employees (including temporary and contract employees) regarding their obligations under this policy and to provide on-going employee training regarding data security.
b. Ensuring that terminated employees no longer have access to ECSU systems that permit access to sensitive or confidential information resources by timely notification to DIT to disable terminated employees' access.
**c.** Advising on appropriate disciplinary measures in response to a violation of information security policies.

**vii. SECURITY OF THIRD-PARTY ACCESS**

Third parties executing business on behalf of ECSU, in lieu of or in addition to ECSU employees, must agree to follow the information security policies of ECSU. Third parties are expected to protect ECSU information resources to the same degree expected from ECSU employees.

Third parties may only access ECSU information resources where there is a business need, only with approval of information resource owners and the ISO, and only with the minimum access needed to accomplish the business objective. An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to the third party prior to access being granted, with provisions made to grant the access in a secure manner. In these cases, third parties shall be subject to the same policies and practices as other members of the ECSU community, unless an exception is granted by the ISO.

**viii. SECURITY OBLIGATIONS IN CONTRACTS FOR OUTSOURCED SERVICES**

Contracts with third parties for outsourced services must include provisions that govern the handling and proper security of all ECSU information resources. These provisions should clearly define requirements of the third party for protection of ECSU information, and where possible, should provide ECSU the ability to audit the third party as needed in order to ensure information is appropriately protected.

ECSU offices and departments must provide oversight of all outsourced service providers to ensure their policies and practices regarding information protection are consistent with ECSU policies.

Third parties will be audited as needed in order to ensure compliance. ECSU information resources must be protected whether used, housed, or supported by ECSU's workforce or by third parties.

The policy provisions pertaining to contracts will be addressed on a go-forward basis. There is no expectation that existing contracts will be renegotiated to comply with these requirements.

## C. LABELING OF INFORMATION

Information and outputs from systems handling ECSU data should be labeled in terms of their criticality, value, and sensitivity to ECSU. Information Owners are responsible for assigning the appropriate classification to each information resource for which they are responsible, and ensuring the information resource is protected in accordance with that classification.

When creating new documents, the document shall be classified and labeled appropriately based on the information contained within and the intended use of the

document. Where possible and appropriate, each document must contain a header or footer on each page that clearly displays the classification for that document. Existing documents will be labeled when revised.

In the event information is not explicitly classified, it is to be treated as follows:

i. Any data that contains sensitive or confidential elements as defined in Section 4.1.1 shall be classified as *Sensitive or Confidential*.
ii. Other information shall be classified as *Internal Use Only.*
iii. Information made publicly available in any form by the Information Owner shall be classified as *Public*.

Information classification may change after a certain period, and such scenarios should be considered when implementing security controls, as over classification can lead to unnecessary expense. Classification guidelines should anticipate and allow the classification of any given item of information to change over time.

**D. HANDLING OF ASSETS**

ECSU is committed to responsible handling and protection of ECSU information. The classification level determines the information security controls that must be applied to protect an information resource, and the procedures that must be followed when collecting, processing, storing, transmitting, or destroying the information resource. Information Owners and Users must notify the ISO if they discover information is not being adequately protected according to its classification.

*Public* information is information that can be disclosed to anyone inside or outside of ECSU, and therefore does not have any special handling requirements other than typical safeguards to protect it against unauthorized modification, destruction, or loss.

*Sensitive & Confidential and Internal Use Only* information have special handling requirements as described in the table below:

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| **Access** | **A.** Access to information must be limited to ECSU faculty, staff, students, and third parties with a specific need-to-know.<br>**B.** Individuals must sign a written confidentiality agreement.<br>**C.** Access must be authorized on an individual basis.<br>**D.** All requests for access must be approved by the | **1.** Access to information must be limited to ECSU faculty, staff, students, and third parties with a specific need-to-know.<br>**2.** Access may be granted on group/role basis.<br>**3.** All requests for access must be approved by the responsible Information Owner. |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | responsible Information Owner.<br>**E.** Strong passwords must be used and changed regularly. When possible, access should be further protected using multi-factor authentication.<br>**F.** File system access control features must be used to limit access.<br>**G.** The Information Owner must regularly review user access and remove individuals who no longer have a need-to-know.<br>**H.** Access for terminated and transferred individuals must be removed immediately.<br>**I.** Access controls must be reassessed annually and updated as necessary. | **4.** Strong passwords must be used and changed regularly.<br>**5.** File system access control features must be used to limit access.<br>**6.** The Information Owner must regularly review user access and remove individuals who no longer have a need-to-know, or who have been terminated or have transferred.<br>**7.** Access controls must be reassessed annually and updated as necessary. |
| **Clear Desk Policy** | **A.** All papers and physical materials must be cleared from the desk and locked away in a drawer, file cabinet, or file storage room when not in use.<br>**B.** Computer screens must be protected by a password-controlled screensaver when not in use. | **1.** All papers and physical materials must be cleared from the desk when not in use.<br>**2.** Computer screens must be protected by a password-controlled screensaver when not in use. |
| **Labeling** | **A.** Information should clearly display its classification label as well as any associated control statement.<br>**B.** Paper, electronic documents, and electronic data files (e.g. spreadsheets) must display the word “SENSITIVE” or | **1.** Information should clearly display its classification label as well as any associated control statement.<br>**2.** Paper, electronic documents, and electronic data files (e.g., spreadsheets) must display the word “Internal |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | "CONFIDENTIAL" in the header or footer of each page or in a similar manner.<br>**C.** Removable media (USB flash drives, CDs, DVDs, etc.) must be labeled "SENSITIVE" or "CONFIDENTIAL". | Use "Internal Use Only" in the header or footer of each page or in a similar manner.<br>**3.** Removable media (USB flash drives, CDs, DVDs, etc.) must be labeled "Internal Use Only". |
| **Distribution** | **A.** Distribution is limited to only faculty, staff, and third parties with an approved business need-to-know and who have signed a written confidentiality agreement.<br>**B.** Student distribution is limited to only information for which they are the subject. Express written consent must be given by the student to authorize a parent or legal guardian to discuss *Sensitive or Confidential* information. | **1.** Distribution is limited to only faculty, staff, and third parties with an approved business need-to-know.<br>**2.** Student distribution is limited to only information for which they are the subject. |
| **Storing Information on ECSU Systems** | **A.** Information should be stored in secured databases or on secured file servers with file system access control features applied to limit access.<br>**B.** Information must not be stored on portable devices unless encrypted (full-disk) and physical safeguards taken to prevent disclosure or theft. Portable devices must require a valid username and password to access the device.<br>**C.** Information may not be stored on mobile devices | **1.** Information should be stored in secured databases or on secured file servers with file system access control features applied to limit access.<br>**2.** Information should not be stored on portable devices unless encrypted (full-disk) and physical safeguards taken to prevent disclosure or theft. Portable devices must require a valid username and password to access the device. |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | unless encrypted. Access to the device must be password or PIN-protected. Information must be deleted from the device when no longer required.<br>**D.** Information must not be copied to non-ECSU off-line media (e.g. USB flash drives, CDs, DVDs, etc.). Information stored in secured off-line media must be encrypted, labeled "SENSITIVE" or "CONFIDENTIAL", and stored in a secure location. Key/combination access should be limited to authorized individuals. | **3.** Information may not be stored on mobile devices unless encrypted. Access to the device must be password or PIN-protected. Information must be deleted from the device when no longer required.<br>**4.** Information must not be copied to non-ECSU off-line media (e.g., USB flash drives, CDs, DVDs, etc.). Information stored in secured off-line media should be labeled "Internal Use Only" and stored appropriately to prevent unauthorized access. |
| **Storing Information on Personally Owned Equipment** | **A.** Information may not be stored on any personally owned equipment. | **1.** Information may not be stored on any personally owned equipment. |
| **Storing Information on Internet-based Hosting/Storage/Sharing Sites** | **A.** Information may not be stored on/with:<br>i. Third-party file storage sites not managed or approved by DIT.<br>ii. Third-party Cloud backup services not managed or approved by DIT.<br>iii. File/photo sharing sites not managed or approved by DIT.<br>unless approved by ECSU General Counsel, the CIO, and ISO.<br>**B.** Information must be encrypted when stored | **1.** Information may not be stored on/with:<br>a. Third-party file storage sites not managed or approved by DIT.<br>b. Third-party Cloud backup services not managed or approved by DIT.<br>c. File/photo sharing sites not managed or approved by DIT unless approved by ECSU General Counsel, the CIO, and ISO. |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | outside the ECSU environment. | |
| **Storing Printed Information** | **A.** Information should be stored in a locked enclosure (desk drawer, file cabinet, or other secure containers) or in secure file or storage rooms.<br>**B.** Key/combination access should be limited to authorized individuals. | **1.** Information should be stored in folders or binders when not in use to prevent casual disclosure. |
| **Copying** | **A.** Copying must be performed or monitored by an individual authorized for access to the information.<br>**B.** Copies must be protected in the same manner as the original. | **1.** No restrictions on copying for business purposes.<br>**2.** Copies must be protected in the same manner as the original. |
| **Printing** | **A.** Printing must be performed or monitored by an individual authorized for access to the information.<br>**B.** Printer must not be left unattended while printing.<br>**C.** Printed documents must display the information's classification label (either printed or applied manually). | **1.** No restrictions on printing for business purposes.<br>**2.** Printed documents must be promptly collected from the printer.<br>**3.** Printed documents must display the information's classification label (either printed or applied manually). |
| **Email** | **A.** Information may not be sent outside ECSU without a business purpose.<br>**B.** Information may be sent or forwarded to individuals authorized for distribution. The recipient's email address must be confirmed prior to sending.<br>**C.** Messages must be encrypted. | **1.** Information may not be sent outside ECSU without a business purpose.<br>**2.** May be sent or forwarded to individuals authorized for distribution. The recipient's email address should be confirmed prior to sending. |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | **D.** Message text must not contain *Sensitive or Confidential* information but should be sent as an attachment if necessary.<br>**E.** Attachments must display the information's classification label. | **3.** Attachments must display the information's classification label. |
| **Mail and Courier** | **A.** Information may be sent through US or ECSU mail.<br>**B.** Information must be in a sealed envelope and clearly labeled on the outside with appropriate markings such as "Sensitive" or "Confidential" or "To be Opened by Addressee Only". | **1.** Information may be sent through US or ECSU mail.<br>**2.** Information should be in a sealed envelope, or in an inter-office envelope with no special marking if sent within ECSU. |
| **Data transmission** | **A.** Information must be sent over secure channel (VPN, SSL) or through secure file transfer.<br>**B.** Information must be encrypted prior to sending if unable to use secure channel or file transfer.<br>**C.** Information must be stored encrypted at the receiving site. | **1.** Information should be sent over secure channel (VPN, SSL) or through secure file transfer if possible. |
| **Facsimile** | **A.** Faxing is authorized unless prohibited by the control statement.<br>**B.** Faxing to a public fax machine is prohibited. | **1.** Faxing is authorized unless prohibited by the control statement.<br>**2.** Faxing to a public fax machine is prohibited. |
| **Conversation/Telephone** | **A.** Conversations must be limited to authorized individuals with a business need-to-know and who have signed a written confidentiality agreement.<br>**B.** Care must be taken to avoid being overheard, | **1.** Conversations must be limited to authorized individuals with a business need-to-know.<br>**2.** Care must be taken to avoid being overheard, especially in public areas or on conference calls. |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | especially in public areas or on conference calls. | |
| **Voicemail** | **A.** Information must not be left on voice mail systems. | **1.** Information should not be left on non-ECSU voice mail systems. |
| **Visual Disclosure** | **A.** Position documents and screens to prevent inadvertent disclosure.<br>**B.** Secure documents and screens when not in use.<br>**C.** Erase all white boards at the conclusion of meetings. | **1.** Position documents and screens to prevent inadvertent disclosure.<br>**2.** Secure documents and screens when not in use.<br>**3.** Erase all white boards at the conclusion of meetings. |
| **Backup** | **A.** Backups require the same level of protection and handling as the originals.<br>**B.** Backup media must be stored in a secure location.<br>**C.** Backup media must be encrypted if transported outside ECSU. | **1.** Backups require the same level of protection and handling as the originals.<br>**2.** Backup media must be stored in a secure location.<br>**3.** Backup media should be encrypted if transported outside ECSU. |
| **Record Retention** | **A.** Information must be retained and disposed of as required by ECSU record retention policy. | **1.** Information must be retained and disposed of as required by ECSU record retention policy. |
| **Disposal** | **A.** Printed information must be disposed of by placing in locked recycling bins designed for sensitive information or shredded with a cross-cut shredder. Printed information must not be placed in normal office trash cans or non-secure recycling bins.<br>**B.** Magnetic hard drives and USB flash drives must be securely wiped using approved wiping tools/programs prior to re-deploying or sent outside ECSU for maintenance or | **1.** Printed information must be disposed of by placing in locked recycling bins designed for sensitive information or shredded with a cross-cut shredder. Printed information must not be placed in normal office trash cans or non-secure recycling bins.<br>**2.** Magnetic hard drives and USB flash drives must be securely wiped using approved wiping tools/programs prior to re-deploying or sent outside ECSU for |

| Requirement | Sensitive & Confidential | Internal Use Only |
|---|---|---|
| | repair. Magnetic hard drives and USB flash drives must be securely wiped or degaussed using approved tools/programs prior to disposal.<br>**C.** CDs and DVDs must be securely disposed of by shredding, chipping, or breaking the disc into multiple pieces.<br>**D.** Magnetic tape and diskettes must be securely disposed of by degaussing, incineration, or shredding. | maintenance or repair. Magnetic hard drives and USB flash drives must be securely wiped or degaussed using approved tools/programs prior to disposal.<br>**3.** CDs and DVDs must be securely disposed of by shredding, chipping, or breaking the disc into multiple pieces.<br>**4.** Magnetic tape and diskettes must be securely disposed of by degaussing, incineration, or shredding. |
| **Inventory** | **A.** All electronic repositories of information must be identified, documented, and reported to the ISO annually. | **1.** All electronic repositories of information must be identified, documented, and reported to the ISO annually. |
| **Re-/Declassify** | **A.** Information may be raised to *Sensitive or Confidential* by ECSU.<br>**B.** Information may be reclassified or declassified by the Information Owner. | **1.** Information may be raised to *Internal Use Only* by ECSU.<br>**2.** Information may be reclassified or declassified by the Information Owner. |
| **Certification** | **A.** Individuals with access to *Sensitive or Confidential* information must review and acknowledge this policy on an annual basis. | **1.** Individuals with access to *Internal Use Only* information must review and acknowledge this policy on an annual basis. |

## 5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to improve the security maturity in protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

**6. COMPLIANCE / SANCTIONS / ENFORCEMENT**

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate with 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. EXCEPTIONS**

No approved exceptions exist at this time.