ELIZABETH CITY STATE UNIVERISTY
Acceptable Use of Information Resources

1. PURPOSE

The purpose of this policy is to provide direction and guidance to members of the Elizabeth City State University (ECSU) community regarding safe and responsible use of ECSU technology resources and to outline the established standards of acceptable use which govern the campus community. To ensure these shared and finite ECSU information resources are used effectively to further ECSU's mission, each individual has the responsibility to:

A. Use the information resources appropriately and efficiently.
B. Respect the freedom and privacy of others.
C. Protect the confidentiality, integrity, and availability of ECSU information resources.
D. Understand and fully abide by established ECSU policies and applicable laws and regulations.

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.

Only the following properly authorized persons may access ECSU computing facilities (hereinafter "Users"):

A. Undergraduate and graduate students currently enrolled in ECSU courses.
B. Non-degree seeking and special students currently enrolled in ECSU courses.
C. ECSU faculty (full and adjunct), staff, and administration.
D. Designated alumni.
E. Official guests of the Chancellor and ECSU.
F. Individuals formally associated with ECSU, upon verification of the appropriate dean and/or administrator.

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.

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.

Proprietary Information. Information that is not public knowledge and is viewed as the property of the ECSU.

Risk. *The probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.*

Security Breach. An unauthorized intrusion into an ECSU information resource where unauthorized disclosure, modification, or destruction of 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.

Social Media. Websites and applications that enable users to create and share content or to participate in social networking.

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

4. POLICY

ECSU is committed to protecting its information resources from illegal or damaging actions by individuals, either knowingly or unknowingly. ECSU information resources, including

but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and other information services, are the property of ECSU. These systems are to be used for business and scholarly purposes in serving the interests of ECSU in the course or normal ECSU activities. It is the responsibility of Users to know these guidelines, and to conduct their activities accordingly.

A. GENERAL USE AND OWNERSHIP

i. Users with ECSU authorized accounts may use the available computing facilities for official ECSU business and scholarly purposes so long as such use:
   a. Does not violate any law or ECSU policy.
   b. Does not involve significant use of ECSU resources, direct costs, or substantial interference with the performance of ECSU duties/work.
   c. Does not result in commercial gain or private profit.
   d. Does not bring discredit to the ECSU establishment.

ii. Students must read and agree to abide by the terms and conditions of the ECSU Connection Privilege Agreement when connecting a computer to the ECSU network.

iii. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Limited and reasonable personal use is permitted but is subject to all requirements and prohibitions of this policy.

iv. While ECSU desires to provide a reasonable level of privacy to faculty, staff, and students, Users should be aware that the data they create and store on ECSU systems remains the property of ECSU. Because of the need to protect ECSU information assets, ECSU cannot guarantee the individual confidentiality of information created or stored on any computing device belonging to the university.

v. Users may access, use, or share ECSU proprietary information only to the extent it is authorized and necessary to fulfill assigned ECSU job duties.

vi. Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of ECSU proprietary information.

vii. For security and network maintenance/operation purposes, authorized individuals within ECSU may monitor ECSU equipment, systems, and network traffic at any time, in accordance with ECSU policies and procedures.

viii. ECSU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and, in instances of misuse, take appropriate disciplinary measures, including legal action.

B. SECURITY AND PROPRIETARY INFORMATION

i. Information contained on ECSU computing systems should be classified and handled as described in ECSU_ITS_003 Information Classification. Users should take all necessary steps to appropriately protect any confidential information.

ii. Users must keep passwords secure and not share accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

iii. Users are responsible for any activity originating from their account. If unauthorized use is detected, Users must change the account password immediately and report the

incident to the Information Security Office/Officer (ISO) or the Information Technology Client Services (ITCS) Help Desk.

iv. All PCs, laptops, and workstations with access to ECSU information resources must be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. Users must log off or proactively invoke the password-protected screen saver when the device is unattended.

v. Because information contained on portable computers and other smart devices is especially vulnerable, special care to protect these assets should be exercised. Users should ensure these devices are used in accordance with all applicable policies.

vi. All systems that are connected to the ECSU's production network must be adequately protected against compromise by malicious software using a reputable malware protection product configured to:
   a. Be active at all times.
   b. Always scan files when they are opened, executed, or downloaded.
   c. Periodically scan the entire system – memory, hard disk, and USB media.
   d. Remove malware from the system or quarantine affected files.
   e. Automatically contact the vendor's update servers at least once a day to verify signature files and scanning engine are up-to-date and install updates if necessary.

vii. Users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, Trojans, or other forms of malicious software (malware).

C. UNACCEPTABLE USE

The following activities are prohibited. Under no circumstances are Users of ECSU information resources authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing university-owned resources or conducting ECSU business.

The lists below are by no means exhaustive, but rather attempt to provide a framework for activities, which generally fall into the category of unacceptable use.

i. SYSTEM AND NETWORK

a. **Downloading or Distributing Unlicensed Software**. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ECSU and the end user.

b. **Sharing Your Password.** Revealing your account password to any other person or entity or allowing use of your account by any other person or entity (e.g., administrative assistants, graduate assistants, co-workers, classmates).

c. **Unauthorized access.** Accessing data of which the User is not an intended recipient or logging into a server or account that the User is not authorized to access, unless these duties are within the scope of the User's regular ECSU job function.

d. **Disrupting Network Communications.** Interfering with network communications through disruptive activity such as network sniffing, network floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
e. **Circumventing Access Controls**. Bypassing user authentication or authorization access control mechanisms to access or alter ECSU information resources the User is not authorized to access.
f. **Attempting to Intercept, Compromise, or Tamper with Passwords.** Copying password files, password "cracking", installing keystroke logging software, intercepting network traffic, or attempting to discover passwords of other Users to gain unauthorized access to ECSU information resources.
g. **Unauthorized Scanning of Networks or Systems**. Scanning ECSU networks or systems for security vulnerabilities (this includes port scanning) is expressly prohibited unless prior notification to ISO is made.
h. **Monitoring Network Traffic without Permission.** Executing any form of network monitoring which will intercept data not intended for the User's computing device (unless this activity is a part of the User's normal ECSU job duties).
i. **Interfering with Normal Service Operations**. Intentionally interfering with or denying service to any computing device (e.g., denial of service attack).
j. **Interfering with Network Traffic**. Using any tools, or sending messages of any kind, with the intent to interfere with or disable regular network traffic.

ii. IT SYSTEMS

a. **Granting Unauthorized Access**. Granting access to ECSU information resources to unauthorized Users.
b. **Purposefully Downloading Malware**. Introducing malicious programs into ECSU networks or systems (e.g., viruses, worms, Trojan horses, etc.).
c. **Downloading or Sharing Inappropriate Content**. Displaying, procuring, or transmitting material that is in violation of ECSU codes of conduct, sexual or discriminatory harassment policies or laws, or hostile workplace laws.
d. **Using Peer-to-Peer File Sharing Applications**. Using peer-to-peer file sharing applications or websites to upload/download protected intellectual property (e.g., copyrighted video, music, software).

iii. INTELLECTUAL PROPERTY

a. Engaging in Academic Fraud. Using ECSU information resources to engage in academic dishonesty is prohibited by ECSU policy.
b. **Copying Copyrighted Material Belonging to Someone Else**. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ECSU or the end user do not have an active license.
c. Breaching Confidentiality Agreements. Disclosing ECSU proprietary information or data to another party without the consent of ECSU.

d. **Distributing User Information.** Providing information about, or lists of, ECSU Users to parties outside the university.
e. **Violating Export Control Laws**. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. The appropriate ECSU management should be consulted prior to the export of any material that is in question.

iv. EMAIL AND COMMUNICATION

a. **Sending SPAM**. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
b. **Harassment.** Any form of harassment via email, telephone, text messages, instant messenger, or other messaging systems, whether through language, frequency, or size of messages.
c. **Forging Emails**. Unauthorized use, or forging, of email or message header information.
d. **Distributing Chain Emails**. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
e. **Non-business-related Emails.** Sending email messages that are not about a work related or endorsed topic.

v. SOCIAL MEDIA

a. Revealing Proprietary Information. Revealing ECSU confidential or proprietary information or any other material covered by Information Classification & Handling Policy when posting content on social media.
b. Damaging Image or Reputation. Making discriminatory, disparaging, defamatory, or harassing comments when posting content on social media or otherwise engaging in any conduct prohibited by ECSU codes of conduct or policy.
c. Attributing Personal Opinion to ECSU. Representing personal belief and/or opinion as ECSU's on social media. If a User is expressing his or her beliefs and/or opinions on social media, the User may not, expressly or implicitly, represent themselves as an agent of ECSU or use the university's name in a manner that would imply an endorsement of the personal views or activities by the university. Users assume all risk associated with blogging or posting content on social media.

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 / SANCTIONS / ENFORCEMENT

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. EXCEPTIONS

No approved exceptions exist at this time.