FAYETTEVILLE STATE UNIVERSITY

ACCEPTABLE USE OF INFORMATION RESOURCES
(formerly *Use of Computer Resources*)

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:	Revised – October 26, 2021 Revised – October 6, 2017 Revised – September 17, 2010 First Issued – February 2, 2010
Related Policies/ Regulations/Statutes:	●*Information Security* ●*Information Classification and Handling* ●*Information Systems Access Control* ●*End User Information Security*
Contact for Info:	Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to provide direction and guidance to members of the Fayetteville State University (University) community regarding safe and responsible use of University technology resources and to outline the standards of acceptable use members of the University community must abide by. To ensure these shared and University information resources are used effectively to further the University's mission, members of the University community must:

- Use the information resources appropriately and efficiently.
- Respect the freedom and privacy of others.
- Protect the confidentiality, integrity, and availability of University information resources.
- Understand and fully abide by established University policies and applicable laws and regulations.

University employees and students who are found to have violated this Policy may be subject to disciplinary action.

II. SCOPE

This Policy applies to all University employees (regardless of status), students, volunteers and contractors as well as to all other members of the University community. This Policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the University community in connection with University operations. In the event

that any particular information is governed by more specific requirements under other University 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 University computing facilities (Users):

- Undergraduate and graduate students currently enrolled in at least one University course.
- Non-degree seeking and special students currently enrolled in at least one University course.
- University faculty,, staff, and administrators.
- Individuals formally associated with the University, upon approval of the appropriate administrator.

III. DEFINITIONS

The following definitions are used in this Policy:

- **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.

- **Control** shall mean **s**afeguards 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** 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.

- **Proprietary Information** shall mean Information that is not public knowledge and is viewed as the property of the University.

- **Social Media** shall mean **w**ebsites and application that enable users to create and share content or to participate in social networking.

IV. UNIVERSITY OWNED RESOURCES

The University is committed to protecting its information resources from illegal or damaging actions by individuals, either knowingly or unknowingly. University 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 the University. These systems are to be used for business and scholarly purposes in serving the interests of the University in the course or normal University activities. It is the responsibility of Users to know these guidelines, and to conduct their activities accordingly.

A. General Use and Ownership

1. Official/ Personal Use of University Resources

Users with University authorized accounts may use the available computing resources and/or facilities for official University business and scholarly purposes so long as such use:

- Does not violate any law or University policy.
- Does not involve significant use of University resources, direct costs, or substantial interference with the performance of University duties/work.
- Does not result in commercial gain or private profit.
- Does not bring discredit to the University.

Employees and other non-student Users should be aware that the data they create and store on University systems remains the property of the University and may be subject to the NC Public Records Act. Employees may access, use, or share University proprietary information only to the extent it is authorized and necessary to fulfill assigned University job duties.

Employees and other non-student 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.

2. User Responsibility

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

Students must agree to abide by the terms and conditions of the University's policies when connecting a computer to the University's network.

3. Auditing and Monitoring Equipment and Systems

The University 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 actions, to include legal action.

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

B. Information Security

Users of University resources are responsible for the security of information in their possession and will be held responsible for any activity originating from their account. Thus, Users should take all necessary steps to appropriately protect any confidential information by doing the following:

- Keeping passwords secure and not share accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- Immediately change their account password if unauthorized use is detected. Users must report any such incident to the Information Security Office/Officer (ISO) at InfoSec@uncfsu.edu or the Information Technology Services (IT Services) Help Desk.
- Securing all PCs, laptops, and workstations with access to University information resources with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
- Logging off or proactively invoke the password-protected screen saver when the device is unattended.
- Ensuring that special care is used to protect information contained on portable computers and other smart devices. Also, Users should ensure these devices are used in accordance with all applicable policies.
- Use extreme caution when opening email attachments received from unknown senders, which may contain viruses, Trojans, or other forms of malicious software (malware).
- Ensuring that all systems that are connected to the University network be adequately protected against compromise by malicious software using a reputable malware protection product configured to:
    - Be active at all times. Always scan files when they are opened, executed, or downloaded.
    - Periodically scan the entire system – memory, hard disk, and USB media.
    - Remove malware from the system or quarantine affected files. 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.

V. UNACCEPTABLE USE OF UNIVERSITY RESOURCES

Under no circumstances are Users of University 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 University business. Additionally, the following include, but are not limited to, activities the University considers as unacceptable uses of University resources.

A. Activities Affecting the University's Systems and Network

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

2. **Granting Unauthorized Access**. Granting access to University information resources to unauthorized Users.
3. **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 the University and the end user.

4. **Purposefully Downloading Malware**. Introducing malicious programs into University networks or systems (e.g., viruses, worms, Trojan horses, etc.).

5. **Downloading or Sharing Inappropriate Content**. Displaying, procuring, or transmitting material that is in violation of University codes of conduct, sexual or discriminatory harassment policies or laws, or hostile workplace laws.

6. **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).

7. **Playing Graphics-Based Interactive Games**. Due to limited network resources, the use of University network facilities for playing graphics-based interactive games is prohibited.

8. **Effecting Security Breaches.** Accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of the User's regular University job function.

9. **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.

10. **Circumventing Access Controls**. Bypassing user authentication or authorization access control mechanisms to access or alter University information resources the User is not authorized to access.

11. **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 University information resources.

12. **Unauthorized Scanning of Networks/Systems**. Scanning University networks or systems for security vulnerabilities (this includes port scanning) is expressly prohibited unless prior notification to ISO is made.

13. **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 University job duties).

14. **Interfering with Normal Service Operations**. Intentionally interfering with or denying service to any computing device (for example, denial of service attack).

15. **Interfering with Network Traffic**. Using any tools, or sending messages of any kind, with the intent to interfere with or disable regular network traffic.

B. **Intellectual Property**

1. **Engaging in Academic Fraud.** Using University to resources to engage in academic dishonesty.

2. **Using Copyrighted Material without Permission of the Owner**. Unauthorized use of copyrighted materials, 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 the University or the end user does not have permission to use.

3. **Breaching Confidentiality Agreements.** Disclosing proprietary information or data to another party without the consent of the University.

4. **Distributing User Information.** Providing information about, or lists of, University Users to parties outside the University without authorization from the Legal Office.

5. **Violating Export Control Laws**. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. The appropriate University official must be consulted prior to export of any material that is in question.

C. **Email Communications**

1. **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.

2. **Harassment.** Any form of harassment via email, telephone, text messages, instant messenger, or other messaging systems.

3. **Email Spoofing/Forging**. Creation of email messages with a forged sender address.

4. **Distributing Chain Emails**. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.

D. **Social Media**

1. **Revealing Proprietary Information.** Revealing University confidential or proprietary information when posting content on social media.

2. **Damaging Image or Reputation.** Making discriminatory, disparaging, defamatory, or harassing comments when posting content on social media.

3. **Attributing Personal Opinion to the University.** Representing personal belief and/or opinion as the University'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 the University or use the University's name in a manner that would imply an endorsement of the personal views or activities by the University.