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

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

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 Empl.

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

A. Activities $ I I H F W L Q J W K H 8 Q L Y H Q V L W \ ¶ V 6 \ V W H P V D Q G 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 D X W K R U L] H G W R D F F H V V X Q O H V V W K H V H G X W L H V 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 I L O H V S D V V Z R U G ³F U D F N L Q J ´ L Q V W D O O L Q J 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.

D. **Social Media**

1.