FAYETTEVILLE STATE UNIVERSITY

POLICY ON INFORMATION SECURITY

Authority:	Chancellor, Fayetteville State University
Category:	University-wide
Applies to:	Faculty, Staff, and Students
History:	Approved on…. Modified on ….. **Related Policies:** Identity Theft Protection Act of State of North Carolina Network Use Policy Policy on Acceptable Use of Computer Resources Policy on Email Use
Contact for Info:	Chief Information Officer – (672-1477)

I. Purpose

Fayetteville State University maintains electronic information resources which are essential to performing University business. Similar to any other capital resources owned by the University, these resources are to be viewed as valuable assets over which the University has both rights and obligations to manage, protect, secure, and control. University employees, students, and other affiliates are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately. Examples of information resources include, but are not limited to, computer systems, network systems, software and data.

II. Glossary

A. **Information Security Officer** - The Information Security Officer works in conjunction with information resource owners, data administrators, and departmental data security liaisons to insure that access rights to systems and data are consistent and applicable as individuals' jobs require.

B. **Resource Owner** - An administrative officer within the University-given responsibility for managing specific information resources within a functional area. These resources may be equipment-related or data-related.

C. **Resource Steward** - An individual appointed by a Resource Owner to manage a subset of the resources designated as being within the area of responsibility of that Owner.

D. **Resource User** - Any individual requiring access to University information resources in the course of meeting the requirements of the work position or an educational curriculum.

II. Purpose

This policy sets forth the mechanisms by which data stored on University-owned computing systems and utilized by University employees and students is secured and protected. This policy is adopted and promoted in order that:

A. The University can meet its record-keeping and reporting obligations as required by state and federal law, the Board of Trustees, the Board of Governors, and University administrators.

B. The University can comply with the Family Educational Rights and Privacy Act of 1974 (FERPA - the Buckley Amendment) , Identity Theft Protection Act of State of North Carolina and other statutes and policies protecting the rights of individuals.

C. The University can consistently maintain data integrity and accuracy.

D. The University can assure that authorized individuals have timely and reliable access to necessary data.

E. The University can assure that unauthorized individuals are denied access to computing resources or other means to retrieve, modify or transfer data.

F. Every employee, student and affiliate of Fayetteville State University must be aware of these risks, and act in a way to protect the information resources of the University.

III. Scope

This policy applies to all individuals associated with Fayetteville State University, including, but not limited to:

- faculty
- staff
- students
- student assistants
- contractors
- temporary staff

This policy applies to the all University-owned information technology hardware and its software, including, but not limited to, desktop workstations, departmental servers and institutionally available resources, such as:

- servers
- personal computers
- network systems
- access card systems
- computer integrated telephony
- other technology hardware

The policy applies to all University data, and reports derived from University data; and it applies to all programs utilizing University operational data.

III. Responsibilities for Information Security

A. The Chief Information Officer is responsible for ensuring that Fayetteville State University has adequate information security, and that this policy is observed. To that end, the Information Security Officers, currently IT managers, have the added responsibility of developing and publicizing the information security policy, and monitoring its compliance.

B. The Information Security Officers coordinate the standards, procedures, and guidelines necessary to administer access to University information resources. The Information Security Officers work in conjunction with information resource owners, the University Data Administrator, and functional users to develop this material.

C. As expected, every employee, student and affiliate at Fayetteville State University is responsible for protection of University assets, including information systems equipment and data. Each employee, student and affiliate at FSU is responsible for notifying the Information Security Officer whenever he or she observes actions which seem to be contrary to this policy. The Information Security Officer is responsible for responding appropriately to actual or perceived breaches by working together with the Resource Owners and the Information Technology personnel directly responsible for the resource in question.

IV. Passwords

A. Security

1. No one should access University information systems without an authorized network account ID and password. Receiving a network account ID requires approval of the individual(s) responsible for the system in question.

2. A network account ID may be revoked or disabled to protect the system at any time. Network account access will be revoked if the employee, student or affiliate terminates the relationship with the University.

3. Inactive network accounts are temporarily disabled until continued need can be established. Each user is required to change his or her password at least every 90 days. ITTS will automatically enforce this when a user has not changed his/her password within the time of expiration.

4. University applications systems must be configured so that only users with authorized network accounts can access them.

5. Network users logged into systems and computers should not leave their workstations unsecured.

The following password protection guidelines should be followed:

1. Passwords are not to be shared except in emergency circumstances or when there is an overriding operational necessity.

2. Passwords should be changed *immediately* after sharing.

3. Passwords should not be kept in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.

4. Passwords or any other sensitive information are not to be sent via email.

5. Stolen or compromised passwords should be changed immediately

6. Passwords are not to be written down and post it in an unsecured area such as a computer’s monitor.

7. FSU employees are not to provide their user ids and passwords to anyone in person or via e-mail

B. Password Management

All authorized users must enroll in the password management system in order to change and retrieve forgotten passwords. For security reasons, the help desk will no longer be resetting passwords over the phone. Persons not enrolled in the system and need assistance with their password will need to come in person to the help desk with a valid FSU ID.

To enroll in the password management system, network users will need to go to FSU Password Management System.

V. Policy Awareness

A. Every student, employee and affiliate of Fayetteville State University should have access to a copy of this policy. All new students and employees should be made aware of the importance of information systems security and their responsibilities in the process. All effort should be made to include this policy in existing communication mechanisms for policy dissemination.

B. Prior to network accounts being issued, the Resource Stewards of each department are responsible for notifying employees of the security practices of their departments, and the policy of the University.

C. All students must be made aware of the Information Security Policy. The Dean of Students is responsible for notifying students of information security practices relating to students.

D. All affiliates must be made aware of the Information Security Policy. The sponsoring official is responsible for notifying the affiliate of information security practices relating to affiliates.

VI. Access to Equipment

Only authorized persons whose work requires it will be allowed access to information systems resources. All information systems resources will be protected against fire, water, physical damage and theft. The appropriate protection will be selected from among physical barriers, environmental detection and protection, insurance, and other risk management techniques.

VII. Data Protection and Security

All data and program files on University information systems will be protected against unauthorized changes. Sensitive data and program files will be protected against unauthorized reading and copying. FSU requires that all FSU employees save their data files on the network drives instead of the storage on the local PC. Furthermore, employees who make copies of data on thumb drives and CDs must take responsibility to insure that sensitive information such as social security numbers, credit card numbers and addresses of FSU employees and students have additional layers of protection. University information systems shall be configured to control which network accounts can read and/or write to any given file. Every file shall be associated with an owner. The owner of each file is responsible for specifying whether the file is sensitive and which network accounts should be allowed to read and/or write to it.

All university data must be stored in devices that are backed up by the data center. This essentially means that individual users and departments that need to work with university data locally on their workstations must store the data on the network (‘T’ Drive designated for individuals and ‘O’ Drive designated for departments) to protect from inadvertent loss of data. The BANNER system-the ERP system for the campus which houses all student, faculty, and staff information is secured through firewall and backed up nightly at MCNC hosting center for recovery purposes. A copy of the back-up data is physically stored at a MCNC designated off-site location to protect against natural or man-made disasters at the MCNC data center.

VIII. Violations

Violations of this policy incur the same types of disciplinary measures as violations of other University policies including, but not limited to, the revocation or disablement of the network account.

If network account credentials are compromised or unauthorized and sensitive data is discovered on employee desktop computer, laptop, tablet, or other mobile device during routine scan, the following disciplinary measures will incur.

First offense: communication to user and supervisor + disabling of network account + one business day to report to ITTS for mandatory one-on-one training.

Second offense: communication to user and supervisor + disabling of network account + one business day to report to ITTS for mandatory one-on-one training + recommendation of formal write up to be placed on employment records and report to legal.

IX. Revisions

As an ongoing document, the Fayetteville State University Information Security Policy will be reviewed on an annual basis, in cooperation with Resource Owners and Information Technology advisory groups. All affected parties are encouraged to correspond with the Information Security Officer regarding any suggestions for revising this document.