FAYETTEVILLE STATE UNIVERSITY

INFORMATION SECURITY

Authority: Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.

Category: Information Technology

Applies to: ●Administrators ●Faculty ●Staff

History: Issued – October 26, 2021

Related Policies/ Regulations/Statutes:
● *Acceptable Use*
● *Business Continuity and Disaster Recovery*
● *End User Information Security*
● *Human Resource Security*
● *Information Classification and Handling*
● *Information Security Awareness and Training*
● *Information Security Incident Response*
● *Information Systems Operation Security*
● *Information Systems Access Control*
● *Information System Acquisition, Development, and Maintenance*
● *Network Management Security*
● *Physical and Environmental Security*
● *Risk Assessment and Management*
● *Telecommuting Security*

Contact for Info: Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to ensure the protection of Fayetteville State University (University) information resources from unauthorized intrusions, malicious misuse, or inadvertent compromise. This policy establishes the requirements, roles, and responsibilities for ensuring the confidentiality, integrity, and availability of University information resources accessed, managed, and/or controlled by the University.

This Policy establishes the following:

- The University's Information Security Program.
- Processes for ensuring the security and confidentiality of information resources.
- Administrative, technical, and physical safeguards to protect against unauthorized access or use of information resources.
- The assignment of responsibility for the security of departmental, administrative, and other critical University information resources.

- Direction and support for information security in accordance with business requirements and relevant laws and regulations.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Access** shall mean the ability to view, use, or change information in University information resources.

- **Availability** shall mean degree to which information and critical College services are accessible for use when required.

- **Confidentiality** shall mean the 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.

- **End User or Information User or User** shall mean the person or organization that actually uses a product, as opposed to the person or organization that authorizes, orders, procures, or pays for it. End Users include students, faculty, staff, contractors, consultants, and temporary employees.

- **Information Owner** shall mean an **i**ndividual with primary responsibility for overseeing the collection, storage, use, and security of a particular information resource.

- **Information Resource** shall mean data, information, and information systems used by the 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 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** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

- **Risk** shall mean 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** shall mean an unauthorized intrusion into a University information resource where unauthorized disclosure, modification, or destruction of confidential information may have occurred.

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

- **Threat** shall mean an event or condition that has the potential for causing information resource loss and the negative consequences or impact from such loss.

III. INFORMATION SECURITY PROGRAM

The University's Information Security Office/Officer (ISO) will implement the Information Security Program to protect the confidentiality, integrity, and availability of the University's information resources. The Information Security Program will include, but is not limited to, the following activities:

- Development of policies, standards, procedures, and guidelines related to information security.
- Performance of risk assessments of the University's network and systems to identify gaps requiring additional security controls and to provide recommendations to mitigate potential risk.
- Monitoring of the University's network to identify malicious activity.
- Leading security incident response in the event of University information resource compromise or breach.
- Providing security awareness and training to the University community.

IV. INFORMATION SECURITY POLICIES

A. Establishment and Ownership

Policies set a minimum baseline under which the University operates and protects its information resources. Policies will be regularly reviewed and updated to properly reflect changing risk conditions and mitigation techniques. At a minimum, University information security policies will be reviewed annually and updated as required.

The ISO will be responsible for developing information security policies, standards, procedures, and guidelines for the University. The ISO will develop these policies with input and review from University stakeholders, based upon best practices in information security, and in accordance with applicable laws and regulations.

The ISO will collaborate with University leadership to develop information security policies that appropriately address the University's needs. Departments must notify the ISO of issues requiring attention through policy, as well as any needed policy changes.

B. Approval

University information security policies shall be consistent with existing laws, regulations, University culture, and support the University's mission to develop, educate, and serve its community. Policies will be reviewed and approved by University leadership prior to implementation. Once implemented, University employees and students will be notified of the policies and if necessary, provided training.

V. EXCEPTIONS TO POLICIES/PROGRAM

Individuals or units unable to comply with the requirements of the Information Security Program or Policies must submit a written exception request to the ISO for review and consideration. Exception requests must include the scope and duration of the exception, business justification, and a committed remediation plan to achieve compliance. The ISO will review the request to ensure proper consideration has been given to the business needs and benefits, and weighed against the increased security risk to the University. Requests for policy exceptions must be submitted to and approved by the ISO prior to implementation of the requested exception.

In the event of an emergency, members of the University's leadership team shall have the authority to temporarily suspend a specific information security policy in order to recover from a service outage or incident. The University's ISO must be notified of the temporary policy suspension and efforts will be made to compensate for any increased security threat (if necessary).

VI. INFORMATION SECURITY COMPLIANCE, MONITORING, AND ENFORCEMENT

A. Compliance with Information Security Policies and Program

Compliance with the requirements of the Information Security Policies and Program is mandatory for all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the University community, including those affiliated with third parties, who access or in any way make use of University information resources. Individuals must follow the defined requirements and exercise appropriate judgment to ensure the University's information resources are adequately protected. Individuals must only access information resources for which they are authorized. Accessing or attempting to access information resources without authorization is prohibited.

B. Compliance With Legal and Contractual Requirements

University information resources must comply with all applicable laws and contractual obligations. Procedures will be implemented for compliance with statutes and other legal requirements, licensing and other agreements, and intellectual property rights. Procedures will also assure the protection and retention of essential records with retention schedules in accordance with required retention guidelines.

Protection of personal information contained in the University's systems shall meet levels required by legislation and other legal requirements. University employees must ensure information resources are used in accordance with the University's defined policies and procedures.

C. Monitoring

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to ensure the integrity of its information and compliance with information security policies. Individuals should be aware that their privacy is not guaranteed when using University information resources, including use of the Internet or when using University email, telephone, or voicemail.

D. Enforcement

Individuals found to be in violation of University policies will face disciplinary action. The University will consider the severity, impact, and other relevant factors of the violation(s) in determining the extent of discipline. Where a violation of non-compliance of information security policy has occurred, corrective actions and sanctions available to the University include, but are not limited to the following:

- Restriction or suspension of computer access privileges.
- Disciplinary action by their academic division and/or the University up to and including termination/expulsion.
- Referral to law enforcement authorities for criminal prosecution.
- Other legal action, including action to recover civil damages and penalties.

E. Information Security Reviews

To ensure information security is implemented and operated as required in University policies, standards, procedures, and guidelines, the University shall be independently audited at planned intervals or when significant changes within the information technology environment occur.

Additionally, University leadership shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies and requirements as defined in the Information Security Program.

Information systems will be operated and administered in accordance with documented procedures and regularly reviewed and audited for compliance.

VII. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

The University is committed to protecting its employees and students and the University from damaging acts that are intentional or unintentional. It is vitally important that all members of the University community play an active role in ensuring the University's information resources are properly protected. All members must assume responsibility for complying with the University's information security policies. Additionally, the following individuals shall have specific responsibility for ensuring the University's information resources are protected:

A. Information Security Office/Officer (ISO)

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

- Establish, document, and distribute information security polices, standards, procedures, and guidelines.
- Develop and implement a risk assessment process to identify, analyze, and mitigate risks to University information resources.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of violation, breach, or compromise.

- Implement practical and effective technologies and services to ensure the security of University information resources, networks, and computing infrastructure.
- Disconnect any device or disable any account believed to be involved in compromising security of University information resources until the device or account no longer poses a threat.
- Develop and implement an information security awareness program to be offered periodically to all University employees and students.

B. <u>Information Technology Services (IT Services)</u>

Information Technology Services staff have primary operational responsibility for information systems that receive, create, store, handle, or discard information. Information Technology Services shall be responsible for the following:

- Implementing information security technologies, controls, and services to protect information resources as required by the Information Security Program.
- Granting and revoking user rights to information resources and privileged user access to information systems as directed by the ISO or information resource owners.
- Ensuring availability and recovery of information resources.
- Abiding by the requirements of the Information Security Program.

C. <u>Senior Leadership</u>

The University's Senior Leadership (including the Chancellor, Vice Chancellors and other members of the senior leadership team) shall be responsible for protecting all University information resources within their respective units as follows:

- Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
- Determining the proper levels of protection, through consultation/coordination with the ISO, for office or department information resources and ensuring necessary safeguards are implemented.
- Ensuring all information resources used by the office or department are assigned an Information Owner.
- Promoting information security awareness in the office or department and ensuring all staff participate in relevant security and privacy training.
- Ensuring office and department staff understand information security expectations and act reasonably to protect University information resources.
- Ensuring end user access to information resources is appropriate for the user's job function, is administered securely, and is regularly reviewed and audited.
- Ensuring office and department staff compliance with the requirements of the Information Security Program.

D. <u>Employees and Students (Users)</u>

Users shall be responsible for the following:

- Reviewing, understanding, and complying with all relevant University information security policies, standards, procedures, and guidelines.

- Providing appropriate physical security for information technology equipment, storage media, and physical data.
- Ensuring sensitive or confidential information is not distributed or accessible to unauthorized persons.
- Protecting the confidentiality of personal passwords, never sharing under any circumstance.
- Logging off from all applications, computers and networks, and physically securing printed material, when not in use.
- Immediately notifying the IT Services Help Desk and the ISO of any incident that may cause a security breach or violation of information security policy.
- Abiding by the requirements of the Information Security Program.

E. <u>Associate Vice Chancellor for Human Resources</u>

The Associate Vice Chancellor for Human Resources shall be responsible for the following:

- 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.
- Ensuring that terminated employees no longer have access to University systems that permit access to sensitive or confidential information resources.
- Advising on appropriate disciplinary measures in response to a violation of information security policies.

VIII. SECURITY OF THIRD-PARTY ACCESS

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

Third parties may only access University 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 University community, unless an exception is granted by the ISO.

IX. 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 University information resources. These provisions should clearly define requirements of the third party for protection of University information, and where possible, should provide the University the ability to audit the third party as needed in order to ensure information is appropriately protected.

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

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