FAYETTEVILLE STATE UNIVERSITY

INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

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: N/A

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

I. PURPOSE

The purpose of this policy (Policy) is to ensure information security is an integral part of Fayetteville State University (University) information systems and resource lifecycle. This policy establishes minimum guidelines for University Information Technology Services (IT Services) to protect the confidentiality, integrity, and availability of University information resources accessed, managed, and/or controlled by University.

This Policy applies to all information collected, stored or used by or on behalf of any University operational unit. In the event that any particular information at FSU is governed by more specific requirements under other FSU policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict.

II. DEFINITIONS

The following definitions are applicable to this Policy:

- **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.

- **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.

III. INFORMATION SYSTEMS SECURITY REQUIREMENTS

Information security related requirements should be included in the requirements for any new information systems or enhancements to existing information systems. Information security requirements should include the following:

- Be identified through policy and regulation compliance, threat modeling, incident reviews, or vulnerability assessments.
- Reflect the business value of the information resources involved.
- Consider the potential negative impact to the University from lack of adequate security.
- Be integrated early in information systems projects for more effective and cost efficient solutions.
- Be documented and reviewed by all relevant stakeholders.

Additionally, the following information security requirements should be addressed:

- Access provisioning and authorization processes (all End Users, including privileged accounts).
- End User duties and responsibilities.
- Protections for the availability, confidentiality, and integrity of University assets.
- Logging and monitoring needs.
- Criteria for formal testing and acceptance of products into University's environment.

Application services passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Considerations include the following:

- Authentication and authorization processes.
- Authorizations for provision or use of the service.
- Protection requirements for confidential information.
- Safeguards, such as encryption, to protect the availability, confidentiality, and integrity of services and transactions.

Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

IV. INFORMATION SECURITY DEVELOPMENT

Rules for the development of software and systems should be established and applied within the University to ensure services, architecture, software, and systems are built securely, thereby reducing risk, vulnerabilities, and cost. These rules apply to internal development practice as well

as any outsourced development contracted by FSU. Aspects of secure development should consider the following:

- Security of the development environment.
- Secure development methodology and secure coding guidelines.
- Security requirements integrated in the design phase.
- Security checkpoints within project milestones.
- Secure code repositories.
- Version control.
- Application security knowledge.
- Capability to detect, fix, and avoid vulnerabilities.

Changes to systems within the development lifecycle should be controlled through formal change control procedures, which at a minimum should include: the following:

- Documenting agreed authorization levels.
- Ensuring changes are submitted by authorized users.
- Reviewing controls and integrity procedures to ensure they will not be compromised by the change.
- Identifying all software, systems, and information that require change.
- Reviewing security code to minimize the likelihood of known security weaknesses.
- Obtaining formal approval prior to work commencement.
- Ensuring authorized user acceptance prior to implementation.
- Ensuring system documentation is updated and previous versions are archived.
- Maintaining version control of all software updates.
- Maintaining an audit trail of all change requests.
- Updating operating manuals and user procedures as necessary.
- Scheduling implementation to minimize disruption.

When operating platforms (operating systems, databases, and middleware platforms) are changed, critical applications should be reviewed and tested to ensure no adverse impact on the University's operations or security. Notification of operating platform changes should be provided in time to allow appropriate testing and review of information systems and applications occur prior to implementation.

Modifications to vendor software packages should be discouraged and limited to necessary changes only. All changes should be strictly controlled, tested, and documented. If changes are required, the original software should be retained and updates made to a designated copy.

Principles and procedures for engineering secure systems should be established, documented, and applied to information system engineering activities and should be designed into all architecture layers (business, data, applications, and technology) to ensure the availability, confidentially, and integrity of the University's information resources. These principles and procedures should be regularly reviewed to ensure they remain up-to-date in combating new threats and applicable to advances in technologies and solutions applied.

A secure development environment includes people, processes, and technology associated with system development and integration. FSU should assess risks associated with individual system development efforts and establish secure development environments, considering:

- Sensitivity of data to be processed, stored, and transmitted by the system.
- Applicable external and internal requirements, e.g., from regulations or policies.
- Security controls already implemented by the University that support system development.
- Trustworthiness of personnel working in the environment.
- The degree of outsourcing associated with system development.
- The need for segregation between different development environments.
- Control of access to the development environment.
- Monitoring of change to the environment and the code within.
- Storage of backups at secure offsite locations.
- Control over movement of data to and from the environment.

The University should supervise and monitor the activity of outsourced system development, to include the following:

- Licensing arrangements, code ownership, and intellectual property rights related to the outsourced content.
- Contractual requirements for secure design, coding, and testing practices.
- Agreement of an approved approach for analyzing the security of the application.
- Acceptance testing for quality and accuracy of deliverables.
- Agreement on minimum acceptable levels of security and privacy quality.
- Evidence sufficient testing has been applied to ensure the absence of intentional and unintentional malicious content upon delivery.
- Evidence sufficient testing has been applied to guard against the presence of known vulnerabilities.
- Right to audit development processes and controls.
- Effective documentation of the build environment used to create deliverables.

Testing of security functionality should be performed throughout the development process and should include a detailed schedule of activities and expected results under a range of conditions. Testing should ensure the system works as expected and only as expected. The extent of testing should be in proportion to the importance and purpose of the system.

Acceptance testing programs and criteria should be established for new information systems, upgrades, and new versions to include the following:

- Testing of information security requirements.
- Testing of adherence to secure system development practices.
- Testing of received components and integrated systems.
- Use of code analysis tools and vulnerability scans to verify remediation of security-related defects.
- Testing in a realistic test environment to ensure the tests are reliable and the system will not introduce vulnerabilities to the University environment.

V. TEST DATA

Test data should be selected carefully, protected, and controlled. The use of production data containing personally identifiable information or confidential/sensitive data for testing should be avoided. If use of confidential/sensitive data is required, access controls and other safeguards

implemented in production systems must be replicated in the test systems. Additionally the following must occur:

- Authorization is required each time production information is copied to a test environment.
- Production information should be erased from the test environment immediately after testing is complete.
- Copying and the use of production information should be logged to provide an audit trail.