FAYETTEVILLE STATE UNIVERSITY

RISK ASSESSMENT AND MANAGEMENT

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:	Revised – March 27, 2024 (Technical Corrections) Revised – October 26, 2021
Related Policies/ Regulations/Statutes:	●Information Systems Operations Security
Contact for Info:	Vice Chancellor for Information Technology & Chief Information Officer | (910) 672-1200

I. PURPOSE

The purpose of this policy is to establish a process to assess, manage, and remediate risks to Fayetteville State University (University) that result from threats to the confidentiality, integrity, and availability of University information resources. It is the responsibility of all faculty, staff, and students to identify, analyze, evaluate, respond, monitor, and communicate risks associated with any activity, function, or process within their relevant scope of responsibility and authority.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Availability** shall mean the degree to which information and critical University 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.
- **Impact** shall mean the consequences, or effects, of a security incident occurring.
- **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.

- **Probability** shall mean the likelihood, or possibility, of a security incident occurring.

- **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 Event** shall mean a system, service, or network state, condition, or occurrence indicating information security may have been breached or compromised or that an information security policy may have been violated or control may have failed.

- **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 a potential event that may cause harm or loss to the University, or individuals associated with the University.

- **Vulnerability** shall mean a weakness in the University's operating environment that could potentially be exploited by one or more threats.

III. ASSESSING SECURITY RISK

To protect the University from the negative effects of security events or incidents, the University has established a process for analyzing threats and determining the appropriate actions to address or remediate those threats. The process of evaluating and assessing security risk covers the following activities:

A. Risk Identification

The ongoing effort to identify events or issues that may lead to the occurrence of a security incident. Security risks may be identified as part of a formal security assessment process, or on an ad-hoc basis by the University community as part of their normal work responsibilities.

B. Risk Analysis

The process of determining and classifying the likelihood and impact of a given risk. Other considerations in the analysis process may include timeframes of any possible security incidents, existing risk mitigations, and prioritization of risks relative to each other. In a

formal security assessment process, each identified risk should be appropriately analyzed and classified, and this analysis will be documented in the FSU Security Risk Register maintained by University Information Security Office (ISO).

C. Risk Mitigation

Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve University's response to a security incident. Note that depending on the situation, it may be appropriate for an identified risk to be accepted by the University (no mitigation activities undertaken). The ISO will work with the appropriate University department or data owner to determine appropriate mitigation actions. In a formal security assessment process, each identified risk will be reviewed to determine appropriate mitigation activities. The ISO will retain and maintain documentation and assessments.

D. Security Risk Register

The University's Security Risk Register is a central repository for information related to security risks that have been identified by the University. It contains information about the identified security risk (including associated vulnerabilities), the impact and probability of damage or loss associated with the risk, and tracks progress toward addressing the risk or states that the risk has been accepted.

IV. MANAGING SECURITY RISK

The University has established the Risk and Compliance Committee whose members are responsible for identifying, prioritizing, and remediating institutional risks. The Risk and Compliance Committee is made up of the University's senior leadership who are responsible for the following:

- Reviewing information technology matters and addressing issues of importance in information technology governance.
- Discussing emerging information security matters at scheduled meetings.
- Receiving and reviewing reports at least annually, on the University's information security program and information technology security controls from the designated senior officer with information security responsibility.
- Reviewing the University's documentation and assessments

The ISO is responsible for determining when a formal security risk assessment is required for a given system or situation. All University employees are responsible for consulting with the ISO for security risk assessment in each of the following situations:

- Use of an externally hosted system or application (SaaS or Cloud Service Provider) for storing or transmitting FSU information.
- Deployment of any application, system, or service hosted by FSU accessible remotely via the Internet.
- Deployment of any application, system, or service (internal or external) that will house any FSU confidential data.
- Any configuration change to the FSU firewall.

- Any change in process or procedure for handling or interacting with confidential data.
- Any other scenario that may introduce a new security risk to the organization.

Since security threats are constantly changing and evolving, it is important that the University environment be assessed for changes in security risk posture on an ongoing basis. Systems implemented and operated by the University are assessed for vulnerabilities on a periodic basis. See the University's *Information Systems Operations Security* policy for additional information.

Additionally, security assessments must be performed at least annually for the University's data centers and external Internet presence. These assessments must be performed by an independent, third-party security assessment organization. The results of these assessments are to be reviewed by the ISO and appropriate Division of Information Technology Services staff, and any noted security issues must be remediated appropriately.