Policy Summary: The University must implement a security awareness and training program for all faculty, staff and students.

Purpose: This policy reflects our commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.

Policy: Faculty, staff and students who have access to the University information systems must understand how to protect the confidentiality, integrity, and availability of information systems.

The University must develop, implement, and regularly review a formal, documented program for providing security training, education and awareness to its faculty, staff, students, and volunteers.

University faculty, staff, students, and volunteers must be provided with regular training, supporting reference materials, and reminders to enable them to appropriately protect University information systems. Such training may be provided at the University facility or via remote training methods. This training must include, but is not limited to:

- All University information security policies, procedures and standards and/or significant revisions to them.
- The secure use of University information systems (e.g. log-on procedures, authorized software).
- Significant risks to University information systems and data and/or any new threats as they are identified.
- The University’s legal and business responsibilities for protecting its information systems and data. (e.g. HIPAA, business associate contracts) and/or any significant changes to these responsibilities.
- Security best practices (e.g. how to construct a good password, how to report a security incident) and/or changes to these practices.
- Security controls in place, any changes to these controls, and/or new controls being implemented.

As part of this training, University faculty, staff, students, and volunteers must read, confirm their understanding, and agree to comply with the Acceptable Use Policy (AUP) prior to receiving access to University information systems.

University faculty, staff, students, and volunteers must receive appropriate security training and after such training, each employee must verify that he or she has received the training, understood the material presented, and agree to comply with it.

All University information security policies and procedures must be readily available for reference and review by appropriate faculty, staff, students, business associates and third-party workers.
All University workforce members responsible for implementing safeguards to protect information systems must receive formal training that enables them to stay abreast of current security practices and technology.

**Documentation:**
All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.

**Scope/Applicability:**
This policy is applicable to OUHSC.

**Regulatory Reference:**
- HIPAA 45 CFR 164.308(a)(1)(ii)(B)
- 16 CFR Part 314 Standards for Safeguarding Customer Information

**Definitions:**
See the Information Security Policy Definitions document for definitions.

**Responsible Department:**
Each organizational unit within the University of Oklahoma that manages its own information systems is responsible for complying with this policy.

**Enforcement/Audit:**
The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.

**Related Policies:**
Risk Analysis, Data Classification, Resource Identification, Resource Classification

**Renewal/Review:**
This policy is to be reviewed and updated as needed by IT Information Security Services.