Information Security Policy

Purpose

The purpose of this policy is to provide guidance for establishing information security requirements for all information assets and systems under the University's defined control and for any parties who access these systems. Adherence to these requirements ensures that the University of Central Oklahoma ("University", "UCO") protects its information assets with due diligence, complies with government regulatoryand contractual requirements and meets industry best practices for this protection.

Terms and Definitions

Data

Groups of information that represent attributes of variables stored, transmitted and/or processed by information systems.

Information Assets

A definable piece of information recognized as having value to the University.

Malicious code

A computer program that causes undesirable results.

Threats

The danger of attack on one or more systems assets.

Security policies

A statement or statements of how the University intends to protect information and systems assets.

Standards, guidelines, requirements, and practices

Standards, guidelines, requirements, and practices are operable realizations of security policies.

Senior Leadership

The highest managerial level within the University, for example the president, Chief Information Officer ("CIO"), members of President's Cabinet, etc.

System Assets

Information technology software and/or hardware used in conjunction with information assets to fulfill University needs. This includes telecommunication and mobile computer systems.

Scope

This Policy applies to:

1. This policy applies to all divisions, colleges and units established by the University that exercise any information technology function relating to the mission of the University except for those specifically exempted in writing by the senior leadership of the University.
2. This policy applies to University computer and telecommunications systems; faculty, staff, and students; academic and administrative units; affiliated entities, agents, contractors, and volunteers of the University, members of the community who use and/or administer such systems, or any information asset (as defined in this policy) that connects directly or indirectly to any UCO owned, leased, contracted, or operated computer or telecommunication system.

Rationale

1. The ability for UCO to meet the daily needs of the academic, administrative, and research communities is facilitated, in large part, through the use of information assets to meet their diverse requirements (e.g., collaboration, research, communication, etc.). While critical to the business of the University, these assets also introduce risks. The risks and corresponding threats associated with informationtechnology are increasing in both number and variety. Information technology (IT) infrastructures are increasingly complex to implement and administer. The advent ofhacking tools and persons willing to distribute viruses and malicious code have increased the risks to organizations and the assets they are charged to safeguard.
2. University mission-critical functions supported by information systems continue to expand. Although some data and systems may not be classified as mission critical,they nevertheless represent a significant investment in resources, may contain sensitive data, and are efficient methods of providing a wide range of education related services. Coupled with overall system integration and interconnectivity, University systems and networks are increasingly at risk to intrusions, misuse of data, and other attacks from both internal and external sources.
3. A successful security framework is reliant upon strong leadership support and a comprehensive body of effective and efficient information security standards and procedures that:
    a. Promote public trust,
    b. Ensure continuity of services,
    c. Comply with legal and contractual requirements,
    d. Recognize risks and threats, and
    e. Protect systems assets.

Policy Details

1. UCO must provide its faculty, students and staff (to include contractors or other authorized agents with access to University information resources, data or assets) with clear direction for the safeguarding of University information assets.
2. This information security policy establishes the overall intent of the organization to support and promote information security in all its practices.
3. Statements created to support particular elements of the University's information security policy may be incorporated into existing policies, standards, requirements, guidelines, and practices.
4. In support of this policy, additional standards, requirements, guidelines, and practicesmay be created.
5. The Director of Information Security or designee(s), as appointed by the ChiefInformation Officer in the Office of Information Technology, will manage the information security program and governance via an oversight committee.
6. University organizations (e.g., divisions, colleges, units) will be solicited to designate a representative as the local organizational contact to be the liaison with the Directorof Information Security's group for security-related matters.
7. The University, as part of an overall security management strategy, shall develop information security policies, standards, requirements, guidelines, and practices in support of the UCO "Information Security Framework". All information security policies, standards, requirements, guidelines, and practices shall ensure compliance with all federal and state security-related regulations that apply to the University's mission and services. These instruments shall consider organizational risk and business impact within their design and be written to recognize the resource impact and constraints of University organizations.
8. The University shall ensure that faculty, staff, students, and any University partners/affiliates are aware of their specific information security responsibilities in theuse of information systems and the handling of information assets.
9. The University's minimum-security requirements provide the foundation for information security policy development. The core assumptions of these requirementsare adapted from the National Institute of Standards and Technology (NIST) Risk Management Framework and Security Controls and ISO 27001/2 and the State of Oklahoma's Information Security Policy.
10. Risk Management: The University shall apply risk management techniques to balancethe need for security measures considering the cost benefit analysis to make informeddecisions and to aid in designing and implementing any security policies, standards, requirements, guidelines, and practices. Impact upon the teaching, research, andservice mission of the University will be considered as a key factor in this process.
11. Confidentiality, Integrity and Availability: The University shall ensure that its information security policies, standards, requirements, guidelines, and practices address the basic security elements of confidentiality, integrity and availability.
12. Protect, Detect, and Respond: Security policies, standards, requirements, guidelines,and practices shall include methods to protect against, detect, and respond to threatsand vulnerabilities to unit information and systems. These instruments will be implemented with consideration of business impact and resource constraints for all University units tasked with their implementation.
13. Identification and Authentication: The University shall implement identification and authentication requirements for information systems and services that protect the University's data and physical information assets in the most appropriate manner.

14. Access Control and Authorization: The University shall implement access control andauthorization policies, plans, standards, and procedures required to protect system assets and other information resources maintained by its colleges and offices.
15. Security Audit Logging: The University shall implement a security audit logging capability for information systems, including computers and network devices.
16. Security Management and Administration: The University shall implement a University-wide security management and administration program.

Responsibilities

Director for Information Security, Office of Information Technology

1. Coordinate and administer the information security program.
2. Develop and maintain security policies, standards, requirements, guidelines, and practices to ensure information security and the associated action steps to prevent and mitigate fraud.
3. Develop and maintain appropriate training and associated reporting.
4. Periodically review and update the information security program.
5. Provide an annual report on the program effectiveness.
6. Direct creation of instruments (standards, requirements, guidelines, and practices) on specific technical subjects or in specific areas ofsecurity concern to support the intent of this policy.

Divisions, Colleges and Department Leadership

1. Review internal processes; implement standards, requirements, guidelines, and practices as necessary.
2. Update internal control structure or standard operating procedures asappropriate to reflect University guidelines.
3. Annually review internal processes, control structures, and standardoperating procedures for continued compliance with policies, standards, requirements, guidelines, and practices.
4. Provide impact assessment and feedback on standards, guidelines, requirements, and practices governed by this policy.
5. Identify who must complete training and ensure that training iscompleted.
6. Protect identifying information collected in accordance with all University policies.
7. Report proven or suspected disclosure or exposure of personal information in accordance with University policies.

All individuals to whom this policy applies

1. Follow documented internal processes.
2. Provide impact assessment and feedback to the oversight committeeon security standards, guidelines, requirements, and practices.
3. Complete University required security training.
4. Report proven or suspected disclosure or exposure of personal information, financial fraud, suspected, or actual identity theft to supervisor immediately.

Policy Violations

1. Failure to comply with this policy or other University policies will result in disciplinary action, up to and including termination of employment and/or enrollment. All persons to whom these policies, standards, and guidelines are applicable, as stated above, are responsible for adhering to these rules.
2. All supervisory personnel are responsible for ensuring that these policies, standards,and guidelines are adhered to within their respective areas of responsibility. Any usermay report University policy or law violations to their immediate supervisor, representative faculty or school personnel or using UCOMMENT.

Resources

Related Policies, Standards, and Requirements:

- Data Classification Policy;
- HEOA DMCA Policy; and,
- Privacy Policy.

Information Security Standards and Requirements:

- Access Authorization, and Authorization Management Standard,Acceptable Use of Technology Standard;
- Exception to Information Security Policy Standard;
- Information Assurance and Security Awareness Training Standard,Information Risk Management Standard;
- Network Security Standard; and,
- Permitted Storage and Transmission of PII Standard.

Other:

- State of Oklahoma Information Security Policy,Procedures, and Guidelines https://www.ok.gov/about/security_policy.html
- National Institute of Standards and Technology (NIST)Risk Management Framework, csrc.nist.gov/groups/SMA/fisma/framework.html

---

Submitted by:

Chief Information Officer, Office of Information Technology

Policy Proposal History:

Draft Created: Jan. 17, 2020
Submitted to Cabinet for First Reading
Submitted to Cabinet for Review and Approval
Approved: December 22, 2020