Data Classification Policy

Purpose

The purpose of this policy is to provide a security framework that will ensure the protection of University of Central Oklahoma ("University" or "UCO") information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. University Information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this policy will be developed and published separately.

Terms and Definitions

Term	Definition
Data	Groups of information that represent attributes of variables stored, transmitted and/or processed by information systems.
Availability	The function of establishing an individual's privilege levels to access and/or handle information.
Confidentiality	Ensuring that information is kept in strict privacy.
Integrity	Ensuring the accuracy, completeness, and consistency of information.
Unauthorized Access	Looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.
University Information	Information that UCO collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

Scope

This Policy applies to:

1. This policy applies to all divisions, colleges and units established by the University of Central Oklahoma that exercise any information technology function relating to the mission of the University except for those specifically exempted in writing by the President 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 the Information Security 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 information technology are increasing in both number and variety. Information technology (IT) infrastructures are increasingly complex to implement and administer. The advent of hacking 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.

Policy Details

1. The University 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 data.
2. This data classification policy establishes the overall intent of the organization to support and promote data classification and data security in all its practices.
3. Statements created to support particular elements of the data classification practice at the University will be organized into existing policies, standards, requirements, guidelines, and practices. Creation of new policies, standards, requirements, guidelines, and practices to support the intent of this policy is allowed.
4. The Director of Information Security or designee(s), as appointed by the Chief Information Officer in the Office of Information Technology, will manage the data classification policy.

5. Documents classified as either Restricted or Confidential (as described below) shall have the appropriate classification level noted on each page.

Classification Levels

All University Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

1. RESTRICTED

The following University Information is classified as Restricted:

a. Social Security numbers
b. Bank account, credit card/debit card numbers
c. Driver's License, state, government ID numbers
d. Student education and financial records, including UCO ID/Banner/student ID numbers
e. Information protected by the HIPAA Privacy Rule, under the Americans with Disabilities Act (e.g., individuals' medical records and other individually identifiable health information), or the Family Educational Rights and Privacy Act (FERPA).
f. Other identifiers or records (as defined by State or Federal Law)

State and Federal laws require that unauthorized access to, or disclosure of, certain Restricted information must be reported to the appropriate agency or agencies. **Any reporting of this nature to external parties must be done by or in consultation with the Office of the General Counsel and the Office of Information Technology (OIT) – Information Security Department (ISD) at the Service Desk, or by phone at (405) 974-2255.**

SHARING RESTRICTED INFORMATION:

Sharing of Restricted information within the University may be permissible, if necessary, to meet the University's legitimate business needs. Restricted data elements are subject to specific sharing methods. Any sharing of Restricted information within the University must comply with this and other applicable University policies. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), Restricted information may not be disclosed to parties outside the University, including contractors, without the proposed recipient's prior written agreement; the proposed recipient must agree:

a. To take appropriate measures to safeguard the confidentiality of the Restricted information.
b. Not to disclose the Restricted information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena.

c. To notify the University Office of General Counsel in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification.
d. The proposed recipient must abide by the requirements of this policy.

2. CONFIDENTIAL

University Information is classified as Confidential if it falls outside the Restricted classification but is not intended to be shared freely within or outside the University due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include:

a. Non-Restricted info in personnel files.
b. Donor records.
c. Internal memos, emails, forms, and non-public business documents.
d. Information governed by non-disclosure agreements.
e. Attorney-client communications.
f. Digital copies of signatures.
g. Information obtained via a UCO system requiring a username and password.

SHARING OF CONFIDENTIAL INFORMATION:

Sharing of Confidential information may be permissible, if necessary, to meet the University's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside the University, the proposed recipient must agree:

a. To take appropriate measures to safeguard the confidentiality of the information.
b. Not to disclose the information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena.
c. Notify the University in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification.
d. The proposed recipient must abide by the requirements of this policy.

3. UNRESTRICTED INTERNAL

University Information is classified as Unrestricted Internal if it falls outside the Restricted and Confidential classifications but is not intended to be freely shared outside the University.

The presumption is that Unrestricted Internal information will remain within UCO. However, this information may be shared outside of UCO if necessary, to meet the University's legitimate business needs, and the proposed recipient agrees not to re-disclose the information without the University's consent.

4. PUBLIC

University Information is classified as Publicly Available if it falls outside the Restricted, Confidential or Unrestricted Internal classification..

Protection, Handling, and Classification of Information

1. Based on its classification, University information must be appropriately protected from unauthorized access, loss and disclosure.

2. Handling of University Information from any source other than UCO may require compliance with both this policy and the requirements of the individual or entity that created, provided or controls the information. If you have concerns about your ability to comply, consult the Office of the General Counsel.

3. When deemed appropriate, the level of classification may be increased, or additional security requirements imposed beyond what is required by the Data Classification Policy.

Responsibilities

1. All UCO faculty, staff, students (when acting on behalf of the University through service on University bodies), and others granted use of University Information are expected to:

    a. Understand the information classification levels defined in the Data Classification Policy.
    b. As appropriate, classify and label the information for which one is responsible accordingly.
    c. Access information only as needed to meet legitimate business needs.
    d. Not divulge, copy, release, sell, loan, alter or destroy any University Information without a valid business purpose and/or authorization.

e. Protect the confidentiality, integrity and availability of University Information in a manner consistent with the information's classification level and type.
f. Handle information in accordance with this policy and any other applicable University standard or policy.
g. Safeguard any physical key, ID card, computer account, or network account that allows one to access University Information.
h. Discard media containing UCO information in a manner consistent with the information's classification level, type, and any applicable University retention requirement.
i. Contact the Office of the General Counsel prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.
j. Contact the appropriate University office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

Policy Violations

1. Disciplinary action for violating this policy shall be governed by, but may not be limited to the applicable provisions of the Regional University System of Oklahoma Policy Manual, the UCO Code of Student Conduct, the UCO Employee Handbook, the UCO Faculty Handbook, the Oklahoma State Regents for Higher Education and state and federal laws. Persons who violate this policy may have their access privileges to UCO computing and networking systems revoked and/or other disciplinary action, including but not limited to termination of employment or enrollment.

2. All supervisory personnel are responsible for ensuring that employees whom they supervise complete all required training related to this policy and for reporting suspected violations of this policy to the UCO Office of Information Technology and the UCO Office of People and Culture. Any user may report University policy or law violations to their immediate supervisor, representative faculty or school personnel or using UCOMMENT (https://broncho2.uco.edu/ucomment/main_menu).

Resources

Related Policies, Standards, and Requirements:
Information Security Policy,
Privacy Policy,
Technology Acceptable Use Policy

Information Security Standards, Requirements, Guides, and Summaries:

Approved:

Andrew K. Benton

Andrew Benton, President

Date: June 13, 2023