**COLLEGE POLICY: 471**

## DATA CLASSIFCATION, PROTECTION, AND RETENTION STANDARDS

Purpose and Overview

As an employee of UA Cossatot, you have access to data and sensitive information about students and employees, including personally identifiable information (PII). PII is information that can be used on its own or in combination with other information to identify a specific individual. PII includes names, addresses, phone numbers, social security numbers, passport information, genetic profiles, academic information, healthcare information, employment records, etc. Breach or loss of data in higher education can be very costly and largely depends on the type and amount of data breached. The cost of a data breach can reach millions of dollars and can result in the loss of state/federal funding, including Title III/Title IV funds.

Policy Scope

This policy applies to:

a. All employees, students, contractors, third-party vendors who access institutional systems and data.
b. All information created, received, maintained, or transmitted using institutional systems and data.
c. All devices used to access institutional systems and data.

Roles and Responsibilities

IT staff is responsible for the following:

a. Determine and execute the appropriate data protection procedures to comply with this policy.

b. Determine and implement appropriate security controls, policies, and procedures for hardware, software, and related technologies.

c. Monitor operations as it relates to data protection and backup procedures.

d. Perform periodic testing of data recovery capabilities.

e. Keep all systems updated and patched.

f. Ensure all employees have access to the training required to stay informed on relevant data protection and security standards.

Data owners and users are responsible for the following:

Leadership and department heads are responsible for:

a. Determine appropriate access levels assigned to users.
b. Ensure the data they use is appropriately classified and labeled.
c. Ensuring compliance with data protection requirements.

All users are responsible for:

d. Protecting their credentials and devices from unauthorized access.
e. Handling institutional data according to its classification level.
f. Reporting suspicious activity and security incidents to leadership immediately.
g. Complete mandatory security awareness training.
h. All employees have a responsibility to ensure that all personal data:

    a. Is obtained fairly and stored securely.
    b. Is kept confidential and is not disclosed to unauthorized personnel or third parties.
    c. Is used and shared both appropriately and legally.
    d. If applicable, is disposed of properly when no longer required.

Compliance and Regulation

As an institution of higher education, we must comply to the guidelines set forth in the following privacy regulations and laws:

- Family Education Rights and Privacy Act (FERPA) - Designed to protect students and their families by ensuring the privacy of student educational records. If you have been assigned access to student information, you need to be aware of FERPA regulations and the consequences of violating FERPA regulations. The Family Educational Rights and Privacy Act of 1974 (as amended), sets forth requirements regarding the privacy of student records. This law applies to post-secondary institutions as well as K-12 schools.

- Gramm-Leach Bliley Act (GLBA) - Imposes privacy and information security provisions on financial institutions; designed to protect consumer financial data. Although we are not a financial institution, it was determined in 2017 by the federal Office of Management and Budget (OMB) and the Department of Education's Federal Student Aid (FSA) that colleges and universities must follow the GLBA safeguard guidelines. GLBA compliance will be included in any FSA audits.

- General Data Protection Regulation (GDPR) - is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

- Personal Information Protection Act (PIPA) - Applies to businesses, state agencies, and other entities that acquire, own, or license personal information about Arkansas residents. It requires entities to implement reasonable security measures to protect personal information

from unauthorized access, use, or disclosure.

- Arkansas Personal Data Protection Act (APDPA) - The APDPA applies to entities that conduct business in Arkansas or target Arkansas residents and control or process data of 25,000+ Arkansas customers and/or derive 50% of gross revenue from selling personal data of 10,000+ consumers. APDPA also requires state agencies to ensure digital accessibility. Compliance with ADA Title II and WCAG 2.1 Level AA guidelines.

The need to protect the privacy and integrity of our data requires that all access to the Student Information System (SIS)/Enterprise Resource Planning (ERP), at any level, be limited only to those users with a legitimate need-to-access. All user accounts will be created based on the principal of least privilege. Following this principle means that the least level of access, or permissions necessary to do a job or task, will be granted to a user.

Please consider the following rules to ensure data safety and security:

- Use strong, difficult to guess passwords. Use a combination of both upper/lower case letters, numbers, and special characters. Never use the same password for multiple accounts.
- Multifactor authentication (MFA) should be enabled for all users accessing sensitive information.
- Never share your username and password, under any circumstances, with anyone else. This is strictly prohibited and could result in immediate termination.
- Always lock or log out of your computer when leaving your work area. Staying logged in may allow unauthorized users access to sensitive information.
- Any device with access to SIS/ERP data should only be used by employees of the college with a legitimate need to access. Do not allow students, children, family members, community users, etc. to access these devices.
- Adopt and adhere to a clean desk policy. This means passwords are not written down and stored in locations where they are easily accessible to others. Make sure you keep all documents, files, identification cards, etc. that may contain any personally identifiable information (PII) about a student or employee securely locked away in your desk or file cabinet.
- Personal information should never be transported or stored in off-campus locations. Do not save personal information to removable storage devices unless there is a legitimate need, and the external storage device has encryption enabled. Do not leave college owned devices unattended in public locations or in vehicles.
- Devices accessing potentially sensitive or confidential information must have disk drive encryption enabled.
- Remote access to systems must be secured via a virtual private network (VPN). Never use open/public wireless connections to access private information.
- Manipulation of data other than what is required to perform your job duties is strictly prohibited.

Failure to comply with the Data Protection Standards may result in harm to individuals, organizations, or UA Cossatot. The unauthorized or unacceptable use of data, including the failure to comply with these standards, constitutes a violation of UA Cossatot policy and may subject the user to revocation of the privilege to use UA Cossatot systems or disciplinary action, up to and including termination of employment.

Data Classification

Data must be maintained in a secure, accurate, and reliable manner and readily available for authorized use. Data security measures will be implemented to commensurate with the value, sensitivity, and risk involved.

To implement security at the appropriate level, to establish guidelines for legal/regulatory compliance, and to reduce or eliminate conflicting standards and controls, data will be classified into one of the following categories by its sensitivity and criticality:

| Level | Description | Examples | Protection |
|---|---|---|---|
| **Public** | Public data is information to which the public may be granted access in accordance with UA Cossatot policy or standards. | Marketing materials, course catalogs, public research publications | No special protection required |
| **Internal** | Internal data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be any law or other regulation requiring this protection. | Policies, procedures, internal communications, non-sensitive business data | Access restricted to authenticated users |
| **Confidential** | Is data, that if disclosed to unauthorized persons, would be a violation of federal or state laws, college policy, or college contracts. Any file or data that contains personally identifiable information of a trustee, officer, agent, faculty, staff, retiree, student, graduate, donor, or vendor may also qualify as highly sensitive data. | Personnel records, financial data, student records, research data, SSN, payment card data, health records, FERPA-protected education records | Encryption, access controls, audit logging, DLP policies |

Data Sensitivity Labels

Microsoft Purview sensitivity labels must be applied to documents, emails, and data store in Microsoft 365. The following sensitivity labels that correspond to the data classification levels:

- Public: No encryption, no restrictions
- Internal: Accessible only to authenticated institutional users
- Confidential: Encrypted, restricted to specific groups or individuals

Microsoft Purview Information Protection (MIP)

Microsoft Purview Information Protection (MIP) provides encryption, access controls, and visual markings for sensitive documents. Sensitivity labels can be applied manually by users or automatically based on content inspection. Documents marked as Confidential or Restricted are encrypted and can only be opened by authorized users, even if forwarded or downloaded. Rights Management Services track document access and can revoke access to documents that have been shared.

Microsoft Purview Data Loss Prevention

Microsoft Purview DLP policies automatically detect and protect sensitive information across Microsoft 365. The following DLP policies are enforced:

- Student Records Protection: Prevents sharing of student educational records containing Social Security numbers, student IDs, grades, or disciplinary information with external parties
- Financial Data Protection: Blocks transmission of credit card numbers, bank account information, and sensitive financial documents outside the institution
- Health Information Protection: Protects medical records and health information in compliance with HIPAA where applicable
- Research Data Protection: Monitors and controls access to sensitive research data and intellectual property
- Personally Identifiable Information (PII): Detects and protects combinations of name, address, date of birth, and identification numbers

External Sharing Controls

External sharing in Microsoft SharePoint and OneDrive is controlled through sharing policies. The following restrictions apply:

- Confidential and Restricted data cannot be shared with external users without explicit approval
- External sharing requires recipient verification and link expiration
- Anonymous sharing links are prohibited for sensitive content
- All external sharing activities are logged with notifications enabled.

Device and Data Encryption

All college-owned devices must have full disk encryption enabled via Microsoft BitLocker. BitLocker status is managed and monitored by device compliance policies in Microsoft Intune. These policies also enforce BitLocker encryption for removable storage devices connected to college devices.

Security Monitoring and Threat Detection

The college utilizes the Microsoft Defender suite to protect users and endpoints.

- Microsoft Sentinel serves as the institution's security information and event management

(SIEM) platform. Sentinel collects logs from Microsoft 365, Azure Active Directory, endpoints, network devices, and third-party applications. Security analysts monitor Sentinel dashboards for suspicious activities, analyze incidents using built-in and custom detection rules, and coordinate response activities. Machine learning and behavioral analytics identify anomalies and potential threats. Sentinel is configured to provide notifications of any suspect user activity. Logs are stored in Sentinel for 12 months.

- Comprehensive audit logging is enabled across all Microsoft 365 services through Purview Audit. Logs capture user activities, administrative changes, and security events. Audit logs are retained for two years and are searchable through the Purview compliance portal. High-risk activities such as data downloads, permission changes, and external sharing generate real-time alerts.

- Microsoft Defender provides threat intelligence from Microsoft and other intelligence sharing communities. Threat indicators are automatically integrated into security tools to improve detection and prevention capabilities. Security analysts review threat intelligence reports to understand emerging threats relevant to educational institutions

Data Backup and Recovery

Unless otherwise indicated, the following backup and recovery policies will apply.

a. SIS Server/POISE. The SIS server is backed up daily. One copy of the data is backed up remotely to the Jenzabar datacenter. Another copy of the data is backed up to tape, and media is stored offsite in our safe deposit box at Farmers Bank and Trust. Backup tapes are rotated daily with a monthly archive tape also stored in the safe deposit box.

b. Docubase (Document Imaging/Workflow)– Docuabse is backed up daily with three immutable copies stored remotely using the Rubrik Security Cloud backup solution.

c. Windows Servers (Physical and Virtual) – All Windows servers are backed up daily with three immutable copies stored remotely using the Rubrik Security Cloud backup solution.

d. Office 365 Data– Office 365 user data (Exchange Online, SharePoint Online, Microsoft Teams, and OneDrive) is backed up daily with three immutable copies stored remotely using Rubrik Security Cloud backup solution.

e. Network Shares – All file server data is backed up daily with three immutable copies stored remotely using the Rubrik Security Cloud backup solution.

f. Local User Data – User devices are configured to automatically store user data in Microsoft OneDrive. OneDrive is backed up using Rubrik Security Cloud backup solution. Student data is stored in OneDrive and remains available as long as the student account is active. Student data is removed from OneDrive 30 days after account deletion.

Data Rentention and Disposal

Data retention policies are configured through Microsoft Purview to automatically retain and

dispose of data according to legal requirements and institutional needs. The following retention periods apply unless otherwise specified by legal requirements:

| Data Category | Regulatory Agency | Reguired Retention Period | Disposal Action |
|---|---|---|---|
| Student Educational Records | FERPA, State and Federal Requirements | Permanent | None – Data is permanently stored in Student Information System |
| Title IV Federal Grants – PELL, SEOG, etc. | US Department of Education (FSA) | 3 Years from the end of the award year that aid was disbursed | None – Data is permanently stored in Student Information System |
| Federal Student Loans | US Department of Education (FSA) | 3 Years from the end of the award year the student last attended | None – Data is permanently stored in Student Information System |
| Financial Records | State of Arkansas DFA Record Retention Schedule | 3 to 5 Years after the account fully settled or sent to collections | |
| Personnel Records | State of Arkansas DFA Record Retention Schedule | 7 Years after separation of employment | |
| Litigation Hold or Open Audit Data | Federal/State Laws | Indefinite or until legally resolved | Do not purge until holds are officially removed. |
| Grant or Research Data | Grant Specific Guidelins | Follow grant guidelines and requirements or institutional research requirements. | Purge after retention period expires. |

Artificial Intelligence Usage

UA Cossatot shall ensure that all data used in connection with artificial intelligence systems is collected, processed, stored, and transmitted in accordance with established data protection requirements. Only data that has been properly classified, authorized, and minimized for the intended AI purpose may be used, and personal or sensitive information must be deidentified or anonymized whenever feasible. AI tools and workflows must undergo review to confirm that they

do not introduce unauthorized access, data leakage, or misuse of protected information. Following any updates to AI capabilities, data flows, or risk assessments, the organization shall reevaluate and adjust safeguards to maintain compliance, uphold privacy obligations, and preserve the confidentiality, integrity, and availability of all data involved in AI operations.

Microsoft Copilot uses a combination of Microsoft's built-in safeguards and governance controls enabled by the IT department in our Microsoft 365 tenant. Using Microsoft Copilot ensures:

- Our data stays in our tenant. Copilot operates within the boundaries of our tenant. It uses permissions, access controls, and boundaries defined in our tenant.
- Copilot does not use company data to train the underlying AI models.
- Copilot can only access what the signed-in user already has permissions to access.
- Prompts and responses are processed within Microsoft's enterprise-grade security framework, including encryption in transit and at rest.
- Copilot inherits our Microsoft 365 compliance controls – retention policies, data loss prevention, sensitivity labels, audit logs and conditional access policies.

For these reasons, Microsoft Copilot is the recommended AI model

---

**Policy History:**
November 2, 2026
November 7, 2022

---

**PROCEDURE: NONE**