UA Rich Mountain
Policy: Global Privacy
Version: 2026.03.17

Purpose

The University of Arkansas Community College at Rich Mountain (UACCRM) is committed to protecting the privacy, confidentiality, and security of data entrusted to the institution by students, employees, alumni, and partners. This Global Privacy Policy serves as the overarching framework governing how the institution collects, processes, stores, and protects personal and institutional data in compliance with state, federal, and international laws.

Scope

This policy applies to all UACCRM faculty, staff, administrators, student workers, and third-party vendors who access, process, or maintain university data.

Regulatory Compliance

UACCRM adheres to the following privacy and data protection frameworks:

- **FERPA (Family Educational Rights and Privacy Act):** Governs the privacy of student education records and Directory Information.
- **HIPAA (Health Insurance Portability and Accountability Act):** Governs the protection of Protected Health Information (PHI). (*See the UACCRM HIPAA Security and HITECH Policies and Procedures for specific PHI guidelines.*
- **GLBA (Gramm-Leach-Bliley Act):** Governs the protection of student financial aid and banking records.
- **Arkansas FOIA & Arkansas PIPA:** Governs public records disclosures and the protection of Arkansas residents' personal information.
- **GDPR (General Data Protection Regulation):** Where applicable to EU residents interacting with the university.

Data Classification and Governance

All data collected and maintained by UACCRM must be classified and handled according to its risk level (High, Moderate, Low).

- Employees must consult the **UACCRM Data Classification Policy** and the **UACCRM Data Catalog** to understand the specific storage, transmission, and handling requirements for Personally Identifiable Information (PII) and protected records.

Data Retention and Destruction

UACCRM retains data only for as long as necessary to fulfill its educational mission and comply with legal obligations.

- Data must be retained and destroyed in accordance with the **UACCRM Data Retention Policy**.
- Upon the termination of employment, employee data and access will be handled according to the **UACCRM Employee Data Deletion Policy** and the **High Threat Termination Procedure** (if applicable).

Acceptable Use and Security Controls

To protect user privacy, all personnel must adhere strictly to technical and administrative safeguards:

- **Acceptable Use:** Personnel must sign and abide by the **UACCRM Information Technology Acceptable Use Policy**.
- **AI and Emerging Technologies:** Under the **UACCRM AI Policy**, employees and students are strictly prohibited from entering PII, FERPA, HIPAA, GLBA, or GDPR-protected data into Generative AI tools.
- **Device Management:** The use of personal devices for university business is governed by the **UACCRM BYOD Policy**, and the use of university devices abroad is subject to the **UACCRM International Travel Policy**.
- **Access Control:** Access to private data is granted on a "least privilege" basis per the **UACCRM Access Management Policy** and requires strong authentication per the **Default Domain Password Policy**.

Incident Response and Breach Notification

In the event of a suspected data breach or unauthorized disclosure of PII, personnel must immediately notify the IT Department.

- Responses will be coordinated using the **UACCRM Incident Response Plan**.
- In compliance with **Arkansas Act 260 of 2021**, UACCRM will disclose initial reports of cyber security incidents to the Arkansas Legislative Auditor within five (5) business days.
- In compliance with the **Arkansas Personal Information Protection Act (PIPA)**, affected individuals (and the state Attorney General, if applicable) will be notified of breaches involving unencrypted PII within forty-five (45) days of discovery.

Revision History

Version	Published	Author	Description
2026.03.17	2026.03.17	Bryan Carnahan	Original