UNIVERSITY
of ARKANSAS
AT PINE BLUFF
1873

DATA CLASSIFICATION POLICY

Table of contents

PURPOSE...3

APPLIES TO...3

ROLES AND RESPONSIBILITIES...3- 4

DATA CLASSIFICATION ....5 - 7

POLICY INFORMATION..8

REFERENCES AND RELATED DOCUMENTS..8

Purpose

The University of Arkansas at Pine Bluff community members are responsible for protecting Institutional Data from unauthorized access, modification, or disclosure and are expected to understand and comply with this policy. Data Classification is an established framework for classifying institutional data based on its level of sensitivity, value, and criticality to the University. The classification of data will aid in determining the baseline security controls for data protection.

Applies To

This policy applies to all faculty, staff, students, student employees, volunteers, and contractors who have access to Institutional Data. This policy covers data stored, accessed, or transmitted in any and all formats, including electronic, magnetic, optical, paper, or other non-digital formats. Except for those data classes expressly protected by statute, contract, or industry regulation, the data classification examples presented below are guidelines. The data owner and stewards are ultimately responsible for classifying data under their management. Classifications for particular data sets may be adjusted based on risk assessment or documented business needs.

Roles and Responsibilities

Data Owner — the Executive Cabinet member with organizational responsibility for the University Information Systems and/or Institutional Data used and maintained within their division.

- Review and recommend strategies to implement information security policies.
- Analyze the business impact of proposed strategies.
- Approve proposed strategies.
- Advocate the accepted strategies within their respective division.
- Consult with appropriate parties on the review and approval of information security policy exceptions.

Data Steward — a senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data

- Assign an appropriate classification to Institutional Data.
- Assign day-to-day administrative and operation responsibility for Institutional Data to one or more Data Custodians.
- Approve standards and procedures for day-to-day administrative and operational management of Institutional Data.
- Ensure Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of Institutional Data.
- Understand and approve how Institutional Data is stored, processed, and transmitted by the University and third-party agents of the University.

- Define risk tolerance related to security threats that impact the confidentiality, integrity, and availability of Institutional Data.
- Understand how Institutional Data is governed by university policies, state and federal regulations, contracts, and other legally binding agreements.

Data Custodian — an employee of the University who has administrative and/or operational responsibility over Institutional Data

- Understand and report on how Institutional Data is stored, processed, and transmitted by the University and third-party agents of the University.
- Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of Institutional Data.
- Document and disseminate administrative and operational procedures to ensure consistent storage, processing, and transmission of Institutional Data.
- Access to Institutional Data as authorized by the Data Steward Provision and de-provision.
- Understand and report security risks and how they impact the confidentiality, integrity, and availability of Institutional Data.

Data User — any employee, contractor, or third-party university agent authorized to access the University's Information Systems and/or Institutional Data.

- Adhere to policies, guidelines, and procedures for protecting Institutional Data.
- Report actual or suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to a manager and Director of Technical Services.
- Report actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data to a manager and the Director of Technical Services.

Data Classifications

Data that is created, processed, collected, or maintained by the University are classified into the following three categories:

1. Restricted Data (Confidential)
2. Private Data (Sensitive)
3. Public Data

Restricted Data (Confidential)

a. Data is considered Restricted when their unauthorized disclosure, alteration or destruction would cause a significant risk to the University or its affiliates. Restricted data should only be disclosed to individuals and business partners on a strict need-to-know basis.

b. **Examples:** Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements.

- Payment Card Industry (PCI) data, including credit card numbers, card security codes (CVV2 codes), and authorization codes
- Password, password hashes, encryption keys, and cryptographic tokens used for authentication to a University information system or for the encryption of any other restricted data.
- Personal (unique) identification details, including Social Security Number, driver's license, passport, and student/travel visa numbers
- Health Insurance Portability and Accountability Act (HIPAA) data, including healthcare information and insurance policy numbers
- Magnetic stripes, barcodes, or proximity (RFID, NFC, etc.) data are encoded on identification cards or key fobs and used for authentication, point of sale, or physical security systems.
- Financial account details, including checking, investment, or retirement account numbers.

c. **Transmission and storage** of Restricted data must maintain the highest level of protection.

- Must never be transmitted via email or text.
- Strong passwords and stored on devices that have protection and encryption measures.
- Protected by TS-approved encryption when stored on any device or media that is not physically safeguarded by the University (mobile devices, optical or flash media, etc.)
- Protected by TS-approved encryption when transmitted across public networks such as the internet.

- Protected by multi-factor authentication whenever such capabilities exist.
- Accessed via a TS-approved secure (VPN link) connection when queried from a remote location.
- Stored only on University-owned devices. Confidential data are not permitted to be stored on any personally owned devices, including mobile phones, laptops, or home computers.
- Must be stored only in a locked drawer; a locked room; an area where access is controlled by a guard, cipher lock, and/or card reader; or an area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other individuals not on a need-to-know basis.

Private Data (Sensitive)

a. Data is considered Private when their unauthorized disclosure, alteration, or destruction would cause a moderate level of risk to the University or its affiliates. All institutional data not explicitly classified as Restricted or Public data should be treated as Private data by default.

b. **Examples:** Private data include data that must be guarded due to proprietary, ethical, privacy, or business process considerations. This classification applies even though there may be no legal or contractual controls that require such protection. By default, most administrative data fall into this classification.

   - Admission applications
   - Educational records and information are protected by the Family Educational Rights and Privacy Act (FERPA)
   - Employment applications, personnel files, benefits information, salary, birth dates, and personal contact information.
   - Donor information: personal contact details, donation, and gift amounts that are not disclosed to the public
   - Privileged attorney-client communications
   - Non-public University policies
   - University internal memos and emails, internal reports, budgets, plans, and financial information.
   - Non-public contracts
   - Faculty, staff, and student ID numbers
   - Research data that has not been intentionally released.

c. **Transmission and storage** of Private data require some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the University.

- Protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
- Stored in a closed container (i.e., file cabinet, closed office, or department where electronic door access control systems are in place) to prevent disclosure when not in use.
- Must not be disclosed to parties outside the University without explicit written authorization by an appropriate data owner.
- Must not be stored on any cloud-based information systems not managed or contracted by the University.
- When practical, Private data should only be shared via systems which the University maintains complete administrative control, which includes the ability to remove or modify the data in question.
- Information systems such as web servers must be secured appropriately to prevent the unauthorized modification of published private data.
- Interactive access to databases containing private data should be adequately secured.

Public Data

a. Data are considered Public when their unauthorized disclosure, alteration, or destruction would cause little to no risk to the University or its affiliates. It should be understood that any information widely disseminated within the campus community is potentially available to the public.

b. **Examples:** Public data include data that may or must be freely available to the general public. It is defined as information with no existing local, national, international, or contractual restrictions, access, or usage.

   - Faculty, staff, and student directories
   - Campus maps
   - Course Catalogs
   - Event Calendars

c. **Transmission and storage** of Public data must maintain proper security to prevent its unauthorized modification, unintended use, or distribution.

   - When practical, public data should only be shared via systems which the University maintains complete administrative control, which includes the ability to remove or modify the data in question.
   - Information systems such as web servers must be properly secured to prevent the unauthorized modification of published public data.

- Interactive access to databases containing public data, such as online directories or library catalogs, should be properly secured using query rate limiting, CAPTCHAs, or similar technology to impede bulk downloads or entire collections of data.

POLICY INFORMATION

Continuous improvement. This document's content is subject to regular review based on UAPB Technical Services staff and the campus community's input. Recommendations for development should be submitted to the Director of Technical Services. Continuous improvement. This document's content is subject to regular review based on UAPB Technical Services staff and the campus community's input. The recommendations for development can be submitted to the Director of Technical Services.

REFERENCES AND RELATED DOCUMENTS

Researched on the internet and reviewed various policies online.