UNIVERSITY OF CENTRAL ARKANSAS™ | INFORMATION TECHNOLOGY

Policy Name: Data Classification Policy
Effective Date: 1/1/2023
Revised Date: 1/1/2023
Most Recent Review Date: 1/1/2023

Purpose

UCA uses computer systems to perform education, research, and all other business functions by collecting, storing, and processing data. State, federal, and international laws and regulations require protection of this data and prescribe the types of security and privacy controls required for protecting its confidentiality, availability, and integrity.

The purpose of this policy is to define a data classification schema and define the most effective, efficient, and economically reasonable controls to protect the data.

Scope

This policy applies to all university owned data collected by university business units and departments, stored on university owned devices and systems, transferred between university owned devices and systems or between university owned devices/systems and all other devices and systems owned and operated by third parties who are storing and processing university data.

Policy

I. Data Classification

UCA has developed the following three main classification categories. All data collected, stored, processed and transferred should be categorized and labeled properly. Everyone, including but not limited to faculty, staff, students, and any third party service provider collecting, processing, or storing university data excluding federal, state, and legal institutions (eg: ADHE, DOJ) should implement the security controls defined in this policy.

1. **Highly Sensitive:** Highly sensitive data that, if disclosed to unauthorized persons, would be a violation of federal or state laws, university policy, or university 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 unless the data is already disclosed by the university or classified as public and published on the web sites or public documents, including the directory data as defined by UCA FERPA policy and Arkansas Freedom of Information Act. Highly Sensitive includes all data defined by the state Data and System security standard classifications of Level C (Very Sensitive) and Level D (Extremely Sensitive)[1]. By way of illustration only, some examples of Highly Sensitive data include, but are not limited to:

    - Health information, also known as protected health information (PHI), which includes health records combined in any way with personal information;
    - Names;
    - Addresses;
    - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
    - Any phone numbers, fax numbers, email addresses not listed in university directory and can be used to uniquely identify any individual;
    - Social Security numbers;
    - University identification numbers;
    - Medical record numbers;
    - Health plan beneficiary numbers;
    - Account numbers;
    - Diploma/certificate/license numbers;
    - Vehicle identifiers and serial numbers, including license plate numbers;
    - Device identifiers and serial numbers;
    - Biometric identifiers, including finger and voice prints;
    - Full face photographic images and any comparable images not publicly available; and
    - Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.

[1] https://ssl-dis.ark.org/themes/user/site/default/asset/img/content/DataClassificationGuide.pdf

- Health Information as further defined by the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009,
- Student records (except for that information designated by the university as directory information under Family Educational Rights and Privacy Act) and other non-public student data,
- Payment Card Information (PCI) including cardholder name, service code, expiration date, CVC2, CVV2, or CID value, PIN, and contents of credit card's magnetic stripe
- Certain personnel records such as benefits records, health insurance information, retirement documents and/or payroll records,
- Any data identified by state or federal law or government regulation, or by order of a court of competent jurisdiction to be treated as confidential or sealed by order of a court of competent jurisdiction, and
- Any law enforcement investigative records and communication systems.
- Authentication verifiers including passwords, shared secrets, cryptographic private keys
- GLBA covered financial information including employee payroll and tax data
- Student financial aid information
- IT security information (such as privileged credentials, incident information, device configurations)
- Information covered by GDPR
- Intellectual property
- Unpublished research data

2. **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.

   Internal data is information that is restricted to personnel designated by the university who have a legitimate business purpose for accessing such data. Legitimate business processes include any business process required to perform education and research activities in the university and other supporting activities enabling education and research functions. Much of this data includes any information that is made available through open records requests or other formal or legal processes. Internal data includes all information that is made available under the Arkansas Freedom of Information Act. Internal data includes all data defined by the state Data and System Security standard classification of Level B (Sensitive).[2] By way of illustration only, some examples of internal data include, but are not limited to:

[2] https://ssl-dis.ark.org/themes/user/site/default/asset/img/content/DataClassificationGuide.pdf

- Employment data,
- Business partner information where no more restrictive confidentiality agreement exists,
- Internal directories and organization charts, and
- Planning documents
- Network-System information
- Contracts
- Building plans and associated information
- Export controlled information
- Telecommunications systems information

3. **Public:** Public data is information to which the general public may be granted access in accordance with University of Central Arkansas policy or standards. Public includes all data defined by the state Data and System Security standard classification of Level A (Unrestricted). By way of illustration only, some examples of public data include, but are not limited to:

   - Publicly posted press releases,
   - Publicly posted schedules of classes,
   - Posted interactive university maps, newsletters, newspapers and magazines,
   - Telephone directory information,
   - Information posted on the university's public web site including the web site for Institutional Research and Analytics, and
   - Student records that are designated by the university as directory information under Family Educational Rights and Privacy Act