COLLEGE POLICY: 472

DATA CLASSIFICATION POLICY

Purpose and Overview

College data is information generated by or for and owned by UA Cossatot that is related to college business. College data exists in any format (i.e. electronic, paper) and includes, but is not limited to, all academic, administrative, as well as the computing resources that support the business of UA Cossatot.

To effectively secure college data, there must be a framework in place that describes the data and quantifies the amount of protection required. This policy defines four categories into which all College data can be divided:

- Confidential
- Internal
- Public

Scope

This policy applies to all faculty, staff, student workers, and third-party agents of UA Cossatot as well as any other affiliate who is authorized to access college data.

Policy

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented 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:

1. Confidential Data – 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. 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). 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 one or more of the following data elements about an individual. Health Information as further defined by the Health Insurance Portability and Accountability Act (HIPPA) or the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of

2009, Medical record numbers;

- Student records (except for that information designated by the college as directory information under Family Educational Rights and Privacy Act) and other non-public student data,
- Identifiers such as Social Security numbers or university identification numbers,
- Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.
- Certain personnel records such as benefits records, health insurance information, retirement documents and/or payroll records, Plan beneficiary numbers;
- Payment Card numbers and related elements as defined by the Payment Card Industry and governed by the University of Arkansas payment card policy series (309 series),
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Names;
- Telephone numbers;
- Electronic mail addresses;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Biometric identifiers, including finger and voice prints;
- Face photographic images and any comparable images; and
- 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.

2. Internal Data: 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. 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 University of Arkansas Freedom of Information Policy (207.0). Internal data includes all data defined by the state Data and System Security standard classification of Level B (Sensitive). By way of illustration only, some examples of internal data include, but are not limited to:

- Employment data,
- Business partner information where no more restrictive confidentiality agreement exists,
- Internal directories and organization charts, and
- Planning documents

3. Public: public data is information to which the public may be granted access in accordance with UA Cossatot 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 college's public web site including the web site for Institutional Research, and
    - Student records that are designated by the university as directory information under Family Educational Rights and Privacy Act.

Policy History:
November 7, 2022

PROCEDURE: NONE