Overview

Information and data supporting the mission of the University of Arkansas Community College at Batesville are stored, maintained, and transmitted throughout the UACCB community. Security is integral to this data. Federal and state laws require protection of much of this data. Each of these laws prescribes the types of security and privacy controls required for protecting the confidentiality, availability, and integrity of the data. Consistency and reliability of controls and clarity of responsibility are achieved by developing a framework, which can be applied to any data type.

I. Policy Statement

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.

II. Highly Sensitive Data

Highly Sensitive: Highly sensitive data is information 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 qualifies as highly sensitive data. The highly sensitive classification includes all data defined by the state of Arkansas' "Data and System Security Standard Classifications" as Level C (Very Sensitive) or Level D (Extremely Sensitive). By way of illustration only, some examples of Highly Sensitive data include, but are not limited to the following:

- Health information records, 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:
  - Name
  - Street address, city, county, precinct, zip code
  - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
  - Telephone numbers
  - Fax numbers
  - E-mail addresses
  - Social Security number

Some examples of PHI data elements are listed below:

- Medical record numbers
- Health plan beneficiary numbers
- Vehicle identifiers such as license plate numbers
- Biometric identifiers, including finger and voice prints
- Health Information as further defined by HIPPA (Health Insurance Portability and Accountability Act)
- Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.
- Student records (except for that information designated by the university as directory information under FERPA (Family Educational Rights and Privacy Act) and other non-public student data.
- Unique identifiers such as Social Security numbers or university identification numbers.

- Payment Card numbers and related elements as defined by PCI (Payment Card Industry).
- 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.
- Any law enforcement investigative records and communication systems.

III. Internal Data

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. 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 data defined by the state of Arkansas' "Data and System Security Standard Classification" as 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
- Planning documents.

IV. Public Data

Public: Public data is information to which the general public may be granted access in accordance with University of Arkansas policy or standards. Public data includes all data defined by the state of Arkansas' "Data and System Security Standard Classification" as 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 website
- Student records that are designated by the university as directory information under FERPA (Family Educational Rights and Privacy Act).

V. Responsibilities

This policy is applicable to all university schools, colleges, departments, and other units. The Director for Information Services, at the direction of the Vice Chancellor for Student Affairs, is responsible for establishing appropriate information and data protection policies as well as implementing mechanisms to ensure that protection. The Director for Information Technology Services, at the direction of the Vice Chancellor for Student Affairs, should ensure the following:

- There is appropriate awareness of these data classifications among data owners, data custodians, and, insofar as possible, all data users of UACCB security processes and procedures.
- This data classification policy is available to the University through the UACCB intranet and/or internet.

- University schools, colleges and other units are aware of their responsibilities and responsiveness to ensure that security is effectively accomplished.

VI. Clarifying Points

Continuous improvement. The content of this document subject to regular review based on input from UACCB Information Services staff and the campus community. Suggestions for improvement should be directed to the Director of Information Services.

Adopted: March, 15, 2023