FAYETTEVILLE POLICIES AND PROCEDURES 309.4

Data Classification

I. RATIONALE AND BACKGROUND

Information and data supporting the mission of the University of Arkansas are stored, maintained, and transmitted throughout the immediate and expanded university community. Requirements of and uses for university information are continuously growing and expanding. Access to that information from computers and across networks eases use and expands functionality. Commensurate with that ease of use and functional expansion is the need for appropriate security measures. Security must be integral to those functions.

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 schema, which can be applied to any data type.

II. 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:

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. 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:
  - Names;
  - 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;
    - Telephone numbers;
    - Fax numbers;
    - Electronic mail addresses;
    - Social security numbers;
    - Medical record numbers;
    - Health plan beneficiary numbers;
    - 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;
    - Full face photographic images and any comparable images; and
    - Any other unique identifying number, characteristic, or code that is derived from or related to information about the 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,
- 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,
- Unique identifiers such as social security numbers or university identification 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),
- 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.

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 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.

Public: public data is information to which the general public may be granted access in accordance with University of 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
- Student records that are designated by the university as directory information under Family Educational Rights and Privacy Act.

III. RESPONSIBILITY

This policy is applicable to all university schools, colleges, departments, and other units. The Associate Vice Chancellor for Information Technology Services, at the direction of the Vice Chancellor for Finance and Administration, is responsible for establishing appropriate information and data protection policies as well as implementing mechanisms to ensure that protection. This policy, as well as any other information technology, data protection and management, and security policies, will be updated on a regular basis and published as appropriate.

Specifically, the Associate Vice Chancellor for Information Technology Services should ensure that there is:

- Appropriate awareness among data owners, data custodians, and, insofar as possible, all data users of security processes and procedures,
- Guidelines and mechanisms for data protection practice available to University constituencies, and
- University schools, colleges and other units responsibility and responsiveness to ensure that security is effectively accomplished.

January 2011