Mississippi State University Information Security Program
Data Classification and Individual Responsibilities

1. **Purpose.** The purpose of this section is to establish a classification scheme for official data and information maintained by Mississippi State University and to establish responsibilities for its protection from unauthorized release or modification. To that end, this section assigns responsibilities for the control and appropriate stewardship of such data.

2. **Scope.** The data classification program pertains to stewardship of all data assets at MSU, whether digitized/electronic, in paper form, or spoken. It is directed toward the classification and subsequent protection of information used in the conduct of official business and the representation of data is irrelevant to the requirement to classify and protect it.

3. **Authority.** Federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Privacy Protection Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Intellectual Property Act, the Gramm-Leach-Bliley Act and the Freedom of Information Act require oversight and protection of specific types of data. This program outlines the university recommended procedure to classify and protect data in accordance with applicable Federal and State requirements.

4. **Roles:** The following roles of university personnel are defined below:

    a. **Data User (custodian):** A university employee who has access to official university data as part of his or her assigned duties. Examples of a data user would include a faculty member, a database administrator, an administrative assistant, secretary, student worker, clerk, or office worker, among others.

    b. **Data Manager:** A university official having operational level responsibility for information management related to the capture, maintenance, dissemination, storage and use of data by an organizational entity. Examples of data managers would include the Dean of a College, a Department head, the Chief Human Resources Officer, the Director of Financial Aid, the Registrar, and the Director of Sponsored Programs, among others.

    c. **Senior Official:** University administrators at the Vice President level or equivalent, who have planning and policy level responsibility for data within their areas and management responsibilities for segments of the institutional data.

5. **Data Classification Categories.** Mississippi State University classifies its official university data into three categories – Category I, Category II, and Category III as described in this section.

5.1 **Classifying Data.** The primary consideration in classifying data is damage that would accrue to MSU should the data be inadvertently released to unauthorized parties through any means. Loss of Category I data would do significant harm to the University. Significant harm is a subjective decision criteria to be made by the Senior Official having data oversight, but must include any data whose protection is mandated by Federal or State law or data that would cause irreparable harm to the University or its reputation (e.g., compromise of donor financial holdings or data that would result in a negative image for the University). Loss of Category II data would result in less substantial harm and its protection is not mandated by law. Category II data may require the same or similar protections as Category I data, but its loss or compromise is not deemed unmanageable (e.g., individual student test scores). Category III data is public and requires no protection.

5.2 **General Examples.** Data classification authorities will use the criteria outlined in paragraph 5.1 to decide which classification their data assets fall under. Classification depends on several factors combined with management judgment. To assist in deciding on the appropriate classification, general examples are given below. These are not intended to be comprehensive or definitive. The actual end classification determination is a management decision based on data sensitivity and harm done if the data is inappropriately released or compromised.

a. **Category I data:** Category I data refers to data protected specifically by law or by Mississippi State University policy. Examples of category I data include data covered by HIPAA; FERPA; donor, employee, or sensitive research data; Social Security identification numbers, payment card data; financial institution data, and data that is not otherwise protected by a known civil statute or regulation, but which must be protected due to proprietary, ethical, privacy, or criticality considerations. Specific examples of Category I data include (but are not limited to) the following:

- Social Security numbers
- Credit card numbers
- Patient medical health or record information
- Personal vehicle license/registration information
- Financial records (e.g., financial donor contributions, student/employee financial accounts, bank accounts, aid/grants, fines, or records of financial transactions)
- Personnel records of employees

- Student-specific grade records (including test scores, assignments, and class grades)
- Student transcripts
- Student entry and transfer records
- Access device numbers/passwords (e.g., building access code, Banner passwords, computer passwords, encryption keys)
- Biometric data with personal identifying information
- Human subject information with personal identifying information
- Sensitive research data, including data subject to export control regulations
- Insurance benefit information
- Driver's license number or state identification number

b. **Category II data:** Category II data includes data releasable in accordance with proper authority (Freedom of Information Act, law enforcement investigation) and may include items such as the contents of a specific e-mail containing sensitive information, student date of birth, employee salary. Category II data is that which must be protected due to proprietary, ethical, or privacy considerations. This classification applies to data that is not otherwise protected by a known civil statute or regulation, but if inappropriately released to unauthorized parties could do harm to the university and its reputation. Such release might result in negative publicity. Specific examples of Category II data include (but are not limited to) the following:

- The calendar for a university official or employee
- The emails of a university official or employee containing sensitive information
- Lists of electronic mail addresses
- Promotion and tenure files
- External review letters
- Detailed accreditation results
- Date of birth, place of birth of students or employees
- Internal audit data
- Student evaluations of a specific faculty member
- Findings of internal investigations
- Human subjects research data with no personal identifying information
- Donor giving records
- Minutes of meetings involving personnel decisions
- Records of meetings discussing disciplinary actions

c. **Category III data:** Category III data is general access data. This is data that is not restricted or judged to be Category I or II. This data is subject to

disclosure to all MSU employees as well as the general public. Specific examples of Category III data include (but is not limited to) the following:

- Departmental Web site
- Library data and holdings
- Public phone directory
- Course catalog and curriculum information
- General benefits information
- Enrollment figures
- Publicized research findings
- State budget
- All public information

6. **Responsibilities for Classification of Data.** The overall responsibility for Data Classification rests with the Provost and Executive Vice President. This authority is delegated to the MSU Chief Information Officer. All senior officials at Mississippi State University will require data managers and data users within their scope of responsibility to classify data at Category I, II, or III. The MSU senior official responsible for specific types of data is as shown in Table 1 below.

TABLE 1

Senior Official Data Classification Responsibilities

Data Type	MSU Senior Official
Payroll Data/Financial Data	Vice President for Budget and Planning
Library Data, Student Data, Electronic Records, Course Data, Admissions Data, Scholarships, Financial Aid, Faculty Data, Communications Data, Human Resources Data	Provost and Executive Vice President
Alumni Data, Foundation Data	Vice President for Development and Alumni
Student Medical, Counseling, Housing, Discipline, and University police data	Vice President for Student Affairs

Sponsored Programs, Human Subject Research, Security Clearances, and Security policies	Vice President for Research and Economic Development
Experiment Station, Agricultural, and Veterinary Medicine data	Vice President for Agriculture, Forestry, and Veterinary Medicine
Facilities Data	Vice President for Campus Services
Bulldog Club donor information, athletic financial information	Athletic Director
Other	Provost and Executive Vice President

7. **Data protection measures.** Data classified in Category I or II as defined above or as classified by the appropriate MSU Senior Official will be protected by data users/custodians as follows. It is important in implementing data protection measures to keep in mind that loss of Category I data is more severe than loss of Category II data and may require a higher level of vigilance. Additionally, the below is not intended to be an all encompassing list – it should serve as a starting point and as an example of good protection practices.

    - All U.S. Government classified material must be stored in accordance with procedures approved and implemented by the Vice President for Research and Economic Development.
    - Paper copies of Category I or II data should be secured in locked containers when not in use. Offices containing such data should also be locked when not occupied. A locked office should not be considered sufficient for protection if multiple access keys exist for the office and the office is routinely left open during normal business hours.
    - Verbal disclosure of Category I or Category II data to unauthorized parties is a violation of the MSU data classification program. Employees of MSU must be reminded to discuss such information in protected environments to preserve its confidentiality. This is particularly important when discussing medical information, personnel decisions, student performance, or disability issues.
    - All Category I and Category II paper waste must be shredded or burned. Under no circumstances should such data be discarded in trash cans.
    - Category I or II data must not be displayed in a public area.

- Data managers should strongly encourage a “clean desk” policy in areas where Category I and II data is routinely accessed by users.
- Category I data must be protected by physical access controls and passwords. It is highly recommended that Category I data not be placed on mobile computing devices. However, mobile devices such as laptops and flash drives containing Category I data must employ encryption since these devices are more likely to be lost or stolen.
- Category II data should be protected by physical access controls and passwords wherever possible. It is highly recommended that mobile computing devices containing Category II data employ encryption to the maximum extent possible to protect information in the event of theft.
- Encryption should be employed when electronically transmitting Category I or Category II data.
- The disposal of electronic media containing Category I data is a particular concern. Such media must be electronically wiped clean or destroyed. Electronic media containing only Category II or III information can be locally cleaned before release by data managers or their appointed authority.
- University magnetic media containing unencrypted Category I or II data must not be released to maintenance contractors or leasing agents without first being sanitized.
- Data managers should periodically make data protection measures a matter of interest with their subordinates and oversee the implementation of the data classification program.

8. **Compliance**. The MSU Internal Auditor is responsible for assessing compliance with this program during the course of regularly scheduled audits of university organizations. Requests for Category I or II data from outside sources should be directed to the office of the Chief Information Officer for release authority when an existing process has not been established.