: Data, Information Access, and Security Policy

: 2

: Information Technology Services (ITS)

: June 15, 2024

: Information Technology Services/CIO

---

of the University that exists in electronic, digital, or paper form. The degree of protection required for different types of University Data is based on the nature of the data and compliance requirements. The following three classification levels will be used for classifying University data:

1. **Confidential Data**: Confidential Data is University Data for which unauthorized disclosure or unauthorized modification would result in significant financial loss to the University, impair its ability to conduct business, or result in a violation of contractual agreements or federal or state laws or regulations, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), the State Personnel Act, the Federal Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI DSS). Examples: Social Security Numbers, payment card numbers, medical records, student data that is not considered directory information, information protected by non-disclosure agreements, confidential research data.
2. **Sensitive Data**: Sensitive Data is University Data for which unauthorized disclosure or unauthorized modification would not result in direct financial loss or any legal, contractual, or regulatory violations, but may otherwise adversely impact the University. Sensitive Data is generally intended for use within the University or within a specific unit, department, or group of individuals with a legitimate need-to- know. Examples: Budget and salary

6. Provide incident response coordination and expertise;
7. Monitor networks for anomalies;
8. M

3. Administering Information Custodian-specific business and information protection controls, including information access control;
4. Providing backup and recovery of University Data;
5. Detecting and responding to security violations and vulnerabilities; and
6. Being aware of all relevant University policies and guidelines regarding University Data, including, but not limited to, the Supplemental Regulations to this Policy; and
7. Reporting any suspected or actual policy violations, security breaches or security vulnerabilities to the Information Custodian.

F. **Information Users** include all persons who have been authorized to read, write, or update University Data. Information Users are responsible for:
1. Using University Data in accordance with University policies and guidelines;
2. Maintaining security appropriate for the classification level of University Data during processing or storage of that data;
3. Complying with all security controls established by the Information Custodian and/or Information Manager;
4. Avoiding disclosure of Confidential Data or Sensitive Data to unauthorized persons without the permission of the Information Custodian or Provost/Vice President; and
5. Annually identifying any new databases or information systems which have been created or acquired by them for use by more than one person and that contain Confidential Data or Sensitive Data and reporting such databases or systems to the appropriate Information Custodian.

The Chief Information Officer (CIO) for the Division of Information Technology Services is responsible for developing security procedures and guidelines pursuant to this Policy, ensuring that such procedures and guidelines are published and distributed to all Information Users, and conducting periodic reviews of such procedures and guidelines. This Policy and all supporting procedures and guidelines will serve as the standards of information and data security to be applied by Information Custodians, Information Managers and Information Users and will be the basis for compliance monitoring, review, and audit.

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual.