

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.01 Responsibilities for Information Resources** | **Revised: May 17, 2022** |

1. GOVERNING REGULATIONS

This procedure is governed by the following policies and regulations:

1.1 System Policy [07.01](http://policies.tamus.edu/07-01.pdf) Ethics

1.2 System Policy [33.04](http://policies.tamus.edu/33-04.pdf) Use of System Resources

1.3 System Regulation [29.01.02](http://policies.tamus.edu/29-01-02.pdf) Use of Licensed Software

1.4 System Regulation [29.01.03](http://policies.tamus.edu/29-01-03.pdf) Information Security

1.5 Administrative Procedure [30.02](http://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/3002%20Equipment%20Management.docx) Equipment Management

1.6 Texas Administrative Code (TAC), Title 1, Part 10, [Chapter 202](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards

2. DEFINITIONS

2.1 Information: Any or all data, regardless of form, that is created, contained in or processed by information resource facilities, communication networks, or storage media.

2.2 Information Resources: Computer hardware, peripherals, networks, portable computing devices, storage media, display devices, or any electronic device capable of receiving, storing, managing, or transmitting electronic data. Additionally, it includes software or applications that are designed, built, operated, and maintained to create, collect, record, process, display, or transmit information.

2.3 Information System: An interconnected set of information resources that share a common functionality and are under the same direct management control. An information system normally includes hardware, software, information, applications, and communications.

2.4 Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

2.5 Owner of an Information Resource: A designated department or person responsible for determining controls over and access to an information resource supporting a business function. An owner is responsible and authorized for several tasks:

a. Assigning custody of information resources and providing appropriate authority to implement security controls and procedures;

b. Ensuring accuracy, authenticity and integrity of data;

c. Ensuring compliance with applicable controls;

d. Specifying data control requirements and conveying them to users and custodians.

2.6 Custodian of an Information Resource: A designated department or person responsible for guarding or taking care of an information resource supporting a business function. A custodian is responsible for several tasks:

a. Implementing owner-specified controls and access guidelines;

b. Providing physical and procedural safeguards;

c. Implementing monitoring techniques and procedures for detecting, reporting and investigating security incidents.

2.7 User: A designated department or person authorized to access an information resource supporting a business function. A user is responsible for several tasks:

a. Using the information resource for only approved, job-related purposes;

b. Complying with established controls.

2.8 Major information system: A major information system is any information system that meets one or more of the following criteria:

1. Has development costs of $1 million or more.
2. Requires one year or longer to reach operational status.
3. Involves more than one state agency.
4. Substantially alters work methods of state agency personnel or the delivery of services to clients.
5. Routinely stores or processes confidential data, as in a student information system, on-card system, e-commerce system involving credit card or ACH information, personnel system, or payroll system.
6. Will be used by management for significant financial, personnel, or strategic decisions or enables significant administrative or business processes, such as entity-wide financial accounting system, personnel system for an entity or a large department, management information system for a core business process, database management system supporting administrative functions, e-commerce system, document imaging system for an entity or a division of an entity, one-card system, distance learning system, and customer relationship management system.

3. TYPES OF INFORMATION

3.1 Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state, federal law or other legal agreement. Examples include credit/debit card numbers, bank account numbers, and social security numbers.

3.2 Internal Use: Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws. Examples include institutional budgetary, financial, and operational records such as expenditures, statistics, contracting information, and non-confidential personnel information.

3.3 Public Information: This includes all information made available to the public through posting to public websites, distribution through e-mail, social media, print publications or other media, and information for which public disclosure is intended or required. Examples include published system member documents, organizational charts, statistical reports, fast facts, basic directory information, and educational content available to the public at no cost.

4. AVAILABILITY OF INFORMATION

4.1 Mission Critical: This classification applies to data that requires a high degree of availability for continuity of business operations.

4.2 Non-Critical: This classification applies to data for which unavailability does not significantly affect normal operations.

5. INFORMATION RESOURCES MANAGER RESPONSIBILITIES

5.1 The Information Resources Department Head has been designated as the agency’s Information Resources Manager (IRM) as required by the Texas Department of Information Resources (DIR).

5.2 The IRM is responsible for the following tasks:

a. Establishing procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of agency information resources to protect them against unauthorized access, use, disclosure, disruption, modification, or destruction whether accidental or deliberate.

b. Developing and maintaining Administrative Procedures on information resources management.

c. Monitoring the effectiveness of defined controls for mission critical and sensitive information.

d. Assure availability, integrity, utility, authenticity, and confidentiality of information.

6. DEPARTMENTAL RESPONSIBILITIES

6.1 Departments having ownership responsibilities for information systems (servers, software, applications, databases, and networks) shall:

a. Maintain a security risk management plan and a disaster recovery plan. These plans must be submitted to the Information Resources Department Head for review on an annual basis.

b. Document and maintain a list of information systems based on type and availability of data defined in sections 5 and 6 above. The list should be submitted annually to the Information Resources Department Head.

c. Manage documented processes or procedures for user access, physical access, administrative and special access, authentication methods, and user account management in accordance with TAC Chapter 202.

d. Manage access to files and folders containing applications, databases, or passwords.

e. Ensure compliance with governing regulations identified in section 1 of this procedure and other Administrative Procedures on information resources.

f. Report any security violations regarding improper use, malware, or unauthorized access to the Information Resources Department.

6.2 Departments having custodial responsibilities for information systems (servers, software applications, databases, and networks) shall:

a. Implement a backup solution and process in accordance with Administrative Procedure 50.03 Section 12 to enable recovery of data and applications during disaster recovery situations;

b. Determine the appropriate frequency and extent of data backup(s) to meet needs as defined by the owner;

c. Verify the successful completion of each electronic backup;

d. Test the backup solution at least annually to ensure that the data can be successfully recovered;

e. Implement security controls based on notification from the owner for user access, physical access, administrative access, authentication, and account management;

f. Implement access controls based on notification from the owner to files and folders containing applications, databases, or passwords;

g. Implement security monitoring and health check processes to detect and remediate malware or unauthorized access.

6.3 The Accountable Property Officer (APO) or Alternate Accountable Property Officer (AAPO) is responsible for equipment inventory, including capitalized or controlled information resources assigned to the department or location.

a. Prior to transferring any information resource capable of storing data between departments or reassigning any such information resource between employees, the APO or AAPO must contact the Information Resources Department.

b. The APO or AAPO shall work with the Information Resources Department to assess whether the information resource contains any of the following:

(1) sensitive information – confidential and/or non-public,

(2) mission critical information,

(3) software and/or applications,

(4) other information that is valuable to the agency and/or employee to whom the information resource is currently assigned.

c. Based on this assessment, the APO or AAPO shall follow the instructions provided by the Information Resources Department.

d. The transfer or reassignment shall be completed in accordance with Administrative Procedure 30.02 Equipment Management.

7. HIRING SUPERVISOR RESPONSIBILITIES

7.1 The hiring supervisor shall educate new employees about the importance of information security.

7.2 Supervisors shall ensure that all employees remain aware of and comply with Administrative Procedures on information resources.

8. EMPLOYEE RESPONSIBILITIES

8.1 Employees shall sign the [Information Security Acknowledgement Form](http://tfsfinance.tamu.edu/modules/finance/admin/procedures/Information%20Security%20Acknowledgment%20Form.docx) during new employee orientation.

8.2 Employees shall adhere to governing policies, regulations, and Administrative Procedures on information resources.

8.3 Employees shall be responsible for the physical security of information resources entrusted to them and shall protect these resources from environmental hazards.

8.4 Employees are responsible for information resources assigned to them, whether the resources are inventoried equipment or non-inventory items.

a. Prior to transferring any non-inventory information resource capable of storing data between departments or reassigning any such information resource between employees, the employee must contact the Information Resources Department. This requirement applies to mobile devices, external storage media, etc.

b. The employee shall work with the Information Resources Department to assess whether the information resource contains any of the following:

(1) sensitive information – confidential and/or non-public,

(2) mission critical information,

(3) software and/or applications,

(4) other information that is valuable to the agency and/or employee to whom the information resource is currently assigned.

c. Based on this assessment, the employee shall follow the instructions provided by the Information Resources Department.

d. The transfer or reassignment shall be completed.

9. PRIVACY

9.1 Agency information resources are official State of Texas resources and, as such, are available only for authorized purposes by authorized users.

9.2 All data and files created, sent, received, or stored on information resources owned, leased, maintained, administered, or otherwise under the custody and control of Texas A&M Forest Service may be non-public and are subject to disclosure under the Public Information Act.

9.3 To manage information systems and enforce security, designated employees within the Information Resources Department may access, log, review, or monitor any user activity or any information stored on or passing through the information systems, in accordance with TAC Chapter 202.

9.4. Employees shall have no expectation of privacy in the use of agency information resources, except as otherwise provided by applicable privacy laws.

10. DISCIPLINARY ACTION

10.1 Unauthorized use of information resources is prohibited. Failure to comply with this procedure may result in disciplinary action by the agency.

10.2 Consequences may include administrative actions, such as loss of access privileges, and/or disciplinary actions up to and including termination of employment.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), (979) 458-6607