Information Systems Security Procedures

Division of Finance Computing Services

The following document lists Division of Finance security procedures for Information Systems that are to be followed in order to comply with both ISAAC requirements and SAP 29.01.99.M1 Security of Electronic Information Resources.

Identification of Systems and Responsible Parties:

Information Systems, their Owners, Custodians and Users are identified in the resource registration section of ISAAC for each Department or the Division, where applicable. Unless stated otherwise, the Division of Finance IT Services are considered to be the Custodian of all Information Systems and the Department Head is considered to be the Owner of his or her Department’s Information Systems and data. Users may also be identified in Active Directory by membership in security groups or other Authentication Services such as SSO or CAS relating to specific Information Systems. For all Information Systems, Division of Finance IT Services personnel are considered to be System Administrators and a listing of personnel and job duties is maintained by the Executive Director of IT Services.

Procedures:

Information Owner Responsibilities

The Information Owner and/or his designee(s) shall be responsible for the following:

1. Approve, deny, and review access to Information Systems of both internal and external (vendors) users.
2. Determining the value of Information Systems on an annual basis.
3. Specifying data and security control requirements (access, authentication, etc.), verifying they are in place, and ensuring compliance.
4. Assigning custody of Information Systems to the proper personnel.
5. Confirm that controls are in place classifying the confidentiality, integrity, and availability of data.
6. Specify and ensuring controls are in place based on risk assessment and mitigation procedures.
7. Responsible for defining departmental records retention schedules and ensuring compliance.
8. Assume and approve accountability for exceptions to security controls.

Information Custodian Responsibilities

The Information Custodian(s) shall be responsible for the following:

1. Implementing control(s) specified by the Owner.
2. Providing physical, technical, and procedural safeguards for Information Systems, such as account setup/revocation and physical security of equipment.
3. Assisting the Owner(s) in evaluating the cost-effectiveness of security and audit controls, and monitoring these controls.
4. Implementing monitoring techniques and procedures for detecting, reporting and investigating security incidents. The procedures are as follows, although the order and availability of specific log files will be determined by each specific system and its ability to create the various type of log files:
   a. Review desktop event logs.
   b. Review Information System server event logs.
   c. Review Information System application logs.
   d. Review Information System database logs.
   e. Review Information System firewall logs.
   f. Report security breaches to the proper personnel, which includes Computing and Information Services, the Information System Owner, and the Division of Finance IT Services Executive Director.
5. Implement data changes and tasks in an authorized manner ensuring the integrity of the data, its source, destination, and transmission process.
6. Reviewing security settings and access lists annually.
   a. If employees gain access to Information Systems via their Division of Finance network accounts, his or her account will be disabled upon separation as per Division of Finance procedure.
   b. If an Information System has its own internal user management system, an employee’s account will be disabled upon separation as per Division of Finance procedure unless it is needed for historical or current business purposes, in which case the password will be changed and access to that account approved and documented by the information owner.

7. Informing the Owner when Information Systems are updated.

8. Ensuring quality assurance processes are followed when new security procedures or changes are adopted and getting approval from the Owner before production implementation. Quality assurance procedures include:
   a. Backing up the data prior to upgrade and testing.
   b. Backing up the source code and application prior to upgrade and testing.
   c. Performing a test implementation of the procedure or change.
   d. Investigating any possible negative effects, including but not limited to business interruption, software problems, access problems, or data corruption.

9. Keeping a log of changes (hardware and software) made to the Information System, including how the changes affect security and auditing requirements.

10. Test environments are kept physically or logically separated from production environments on systems where system hardware, functionality, and licensing allow it.

11. Ensuring that all software placed on Information System be appropriately licensed (SAP 29.01.99.M1.05).

12. Ensuring that all Division of Finance IT Services personnel that may assist or act as backup to the Information Custodian are aware of these responsibilities.


System Administrator Responsibilities

The System Administrator(s) shall be responsible for the following:

1. Verifying that the backups are performed by the Division of Finance IT Services according to the IT Services backup documentation and schedule.
   a. Review the backup logs daily for errors or problems with the backups.
   b. Test the backup and recovery system annually.

2. Coordinating updates and changes to Information Systems.
   a. Determine the best time/date for updates to minimize the impact to systems and users.
   b. Determine the inherent risk and mitigating activities, based on possible impact to normal operations.
   c. Minimize the risk of disruption of services.
   d. Obtain owner approval before upgrade/change.

3. Keeping Information Systems users apprised of any relevant issues such as planned down time, software upgrades, or IT procedure changes.

4. In the event of a security incident, the system administrator(s) will
   a. Notify the Information System Owner and the Division of Finance IT Services Executive Director.

5. Assure that all networking infrastructure, configuration, name space, and cabling conforms to State standards and in consultation with the TAMU CIS Networking group.

Approvals:

__________________________________________________________________________  ________________
TAMU Employee Name          Date
Vice President for Finance and CFO

__________________________________________________________________________  ________________
TAMU Employee Name          Date
Executive Director, IT Services