General

The specific roles and responsibilities delineated in this document are intended as a generic set of expectations to guide the management of information technology services and support across Texas A&M University-Kingsville. As with any general guide, there will be exceptions. Exceptions to this rule will be negotiated, documented, and reviewed annually by the head of the unit requesting the exception, other impacted units, and the Chief Information Officer. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles:

CHIEF INFORMATION OFFICER (CIO)

1. Is the University’s Senior Information Technology professional. The CIO reports to the Provost and Vice President for Academic Affairs on all matters relating to Information Resource Management;
2. Ensures availability of information technology systems and operations, including IT contingency planning and IT business continuity planning, to support the University’s mission;
3. Ensures that appropriate security systems and procedures are in place to protect the University’s information and IT equipment assets.
4. Provides IT-related information and reports to state agencies as required by statute as well as to other external agencies and organizations such as the Texas A&M University System and Educause.

INFORMATION SECURITY OFFICER (ISO)

1. Reports directly to the CIO on all matters pertaining to IT security;
2. Develops and maintains the University’s information security program;
3. Provides guidance to personnel with responsibilities for information security;
4. Coordinates the design and implementation of processes and practices that assess and quantify risk;
5. Ensure systems are configured, operated, maintained, and disposed of in accordance with all relevant security guidelines;
6. Is responsible for overseeing configuration and administration of auditing and for ensuring that audit trails are reviewed periodically and archived in accordance with security guidelines;
7. Works closely with System Administrators to ensure all security related functions and activities are performed;
8. Plays a leading role in introducing an appropriate methodology to help identify, evaluate, and minimize risks to all IT systems; and
9. Is responsible to the CIO to ensure that IT systems are configured and maintained securely throughout their lifecycle in accordance with the security policies.
10. Is responsible for developing and recommending policies and establishing procedures and practices, in cooperation with information owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction, or disclosure.
11. Is responsible for monitoring the effectiveness of defined controls for mission critical information.
12. Reports, at least annually, to the CEO or his or her designated representative(s) the status and effectiveness of information resources security controls.
13. With the approval of the CEO or his or her designated representative, may issue exceptions to information security requirements. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.
14. Arranges for a biennial review of the institution’s information security program in compliance with TAC 202.71 by individual(s) independent of the information security program and reports the results to the institution’s CEO or his or her designated representative(s).

INFORMATION OWNER – SYSTEM OWNER

1. The System Owner is the designated senior executive that is responsible for an information system. [Needs format change to the same numbering level as the other sections.]
2. Each System Owner:
   a. Is responsible and accountable for the business aspects of managing a system, including funding and representing the interests of the system throughout its lifecycle;
   b. Ensures system security plans and contingency plans are developed and maintained for each system and applications;
   c. Ensures systems personnel are properly designated, and trained.
   d. Approves access and formally assigns custody of an information resources asset.
   e. Determines the asset's value.
   f. Specifies data control requirements and conveys them to users and custodians.
   g. Specifies appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources and services outsourced by the institution of higher education.
   h. Confirms that controls are in place to ensure the confidentiality, integrity, and availability of data and other assigned information resources.
   i. Assigns custody of information resources assets and provide appropriate authority to implement security controls and procedures.
   j. Review access lists based on documented security risk management decisions.
k. Justifies, documents, and is accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the information security officer or other person(s) designated by the state institution of higher education head.

CUSTODIAN - SYSTEM ADMINISTRATOR

The System Administrator carries out the following activities in accordance with an applicable TAMUK and TAMUS IT policies, rules an administrative procedures:

1. Insures availability of systems for which he or she is responsible as required to carry out the mission of the University.
2. Develops and maintains system security plans and contingency plans for IT systems and major applications for which he or she is responsible;
3. Participates in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies;
4. Installs only hardware and/or software approved by CIS.
5. Installs OS updates and security patches.
6. Implements the controls specified by the information owner(s);
7. Provides physical, technical, and procedural safeguards for the information resources;
8. Assists information owners in evaluating the cost-effectiveness of controls and monitoring; and
9. Implements monitoring techniques and procedures for detecting, reporting, and investigating incidents.

USER

The user must:

1. Adhere to TAMUK Acceptable Use Policy governing the use of information systems;
2. Not download, install, or use unlicensed software on any TAMUK computer;
3. Use e-mail systems in a professional and courteous manner with the understanding that misuse of e-mail will subject them to disciplinary action;
4. Use properly formatted passwords and protects them from unauthorized disclosure.
5. Not use a system or application before receiving appropriate training.
6. Use IT resources only for defined purposes and comply with established controls.

OFFICE OF RESPONSIBILITY: Department of Information Technology

CONTACT: For rule interpretation or clarification, contact Department of Information Technology, Chief Information Officer.

REFERENCES: TAC 202 as amended or supplemented