Procedure:

1. GENERAL

1.1 Texas A&M University-Kingsville’s electronic information resources are vital academic and administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats from both internal and external sources. These threats have the potential to compromise the integrity, availability, and confidentiality of the information.

1.2 Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the University’s information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.

1.3 Texas A&M University-Kingsville, as a state university, is required to comply with the Texas Administrative Code (TAC) on “Information Security Standards”. The Texas Administrative Code assigns responsibility for protection of informational resources to the President. For the purposes of this rule, the authority and responsibility regarding the University’s compliance with the Texas Administrative Code on Information Security Standards has been delegated by the President to the Chief Information Officer (CIO).

2. DEFINITIONS

2.1 Confidential Information - Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records as well as employee records are considered confidential information.

2.2 Mission Critical Information - Information that is defined by Texas A&M University-Kingsville or any division thereof (department, etc.), to be essential to its function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.

2.3 Owner - A person responsible for a University function and for determining controls and access to electronic information resources supporting that University function.
2.4 Custodian - A person (or department) providing operational support for an
information system and having responsibility for implementing owner-defined
controls and access privileges.

2.5 User- The user of the data or record has the responsibility to use the
resource only for the purpose specified by the owner; comply with controls
established by the owner; and prevent disclosure of confidential or sensitive
information.

2.6 ISAAC (Information Security Awareness Assessment and Compliance) - A
web-based system used to assess the security posture of information systems and
measure compliance with the Information Security Standards. It also provides
guides for creating a disaster recovery plan and performing a physical security
check.

3. RESPONSIBILITIES

3.1 The Information Security Officer has been designated as the individual
responsible for administering the provisions of this rule, other applicable
TAMUS and TAMUK rules, and the TAC Information Security Standards.

3.2 The head or director of a department shall be responsible for ensuring that
an appropriate security program is in effect and that compliance with this rule,
other applicable TAMUS and TAMUK rules, and TAC Standards is maintained
for information systems owned and operationally supported by the department.

3.3 The head or director of a department which provides operational support
(custodian) for information systems owned by another Texas A&M University-
Kingsville department shall have the responsibility for ensuring that an
appropriate security program is in effect and that complies
with TAC Standards is maintained for the supported information systems.

3.4 Operational responsibility for compliance with TAC Standards may be
delegated by the department head or director to the appropriate information
system support personnel (e.g. System Administrators) within the department.

3.5 Mission Critical or Confidential Information maintained on an individual
workstation or personal computer must be afforded the appropriate safeguards
stated in the TAC Standards. It is the responsibility of the operator, or owner,
and/or departmental Systems Administrator of that
workstation or personal computer to insure that adequate security measures are
in place.
4. COMPLIANCE ASSESSMENT REPORTING

4.1 Departments having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a security assessment report is filed with the Office of Information Technology (via the ISAAC system). This report is produced by the ISAAC system accessed at http://isaac.tamu.edu/. The report shall be filed by the designated system administrator or custodian of the information system.

4.2 Departments having responsibility for information resources which store, transmit, or process mission critical or confidential information may assess their security posture and measure their compliance with the TAC Information Security Standards by using the Information Security Awareness Assessment and Compliance (ISAAC) system.

OFFICE OF RESPONSIBILITY: Department of Computing and Information Services

CONTACT: For rule interpretation or clarification, contact Computing and Information Services, Information Security Officer or Office Information Technology, Chief Information Officer

REFERENCES: TAC 202 as amended or supplemented