1. GENERAL

Portable computing and storage devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to individuals using the devices. The purpose of this Procedure is to establish the process for the use of portable devices and their connection to the network.

2. APPLICABILITY

This University Procedure applies to all University-owned portable computing devices and all portable computing devices that process, contain, or have direct access to Sensitive Information.

The purpose of the implementation of this University procedure is to provide a set of measures that will mitigate information security risks associated with portable computing. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience is all users of University information resources.

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions. The following definitions apply to this document only.

Portable devices comprise portable computing devices and portable storage devices.

Portable computing device is a computing device which is designed to be easily transported by one person for an extended period. Examples of portable computing devices include laptops, tablet computers, and smartphones.
Portable storage device is an electronic information storage device which is designed to be easily transported by one person for an extended period of time. Examples of portable storage devices include USB memory sticks and USB hard drives.

4. PROCEDURES

4.1. The owner of a portable device connecting to the University network shall ensure that the device adheres to all relevant University procedures relating to information resources, e.g., updating software.

4.2. Users should not store Sensitive Information on any portable device. In the event that there is no alternative to storage on a portable device, users shall encrypt all Sensitive Information using approved encryption techniques (see Procedure 29.01.03.C2.28 – Classification and Protection of Data; Encryption) and store only the encrypted information on the portable device.

4.3. Users shall enable password protection on any portable device that they connect to the University network, or which contains Sensitive Information.

4.4. User may remotely connect to University information resources or Sensitive Information only by methods approved by the IRM.

4.5. The IRM shall approve only those methods for remote access to University information resources or Sensitive Information that encrypt all communications. Examples of such methods are Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), Transport Layer Security (TLS), and Secure Sockets Layer (SSL).

4.6. Custodians of services (e.g., Virtual Private Network or Remote Desktop) that provide remote access to University information resources or Sensitive Information shall ensure that those devices encrypt all communications. Those Custodians shall indicate their compliance with this policy in the annual risk assessment.

4.5. Users of University-owned portable devices must ensure that those devices are physically secure when left unattended. This means those devices shall be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to
this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Office

Office of Responsibility: Office of the Associate VP for Information Technology and CIO