

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.17 Portable Computing

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Portable computing 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 the university's portable computing security procedures is to establish the process for the use of mobile computing devices and their connection to the network.

2. APPLICABILITY

This university procedure applies to all portable information resource devices that process, contain, or have direct access to confidential 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

The intended audience is all users of university information resources.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

4.1. Portable computing devices must adhere to all university procedures relating to information resources. Exceptions may be granted by the Information Resource Manager.

4.2. Sensitive Information should not be stored on portable computing devices. In the event that there is no alternative to local storage, all Sensitive Information must be

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

encrypted using approved encryption techniques and access to the device must be password protected.

- 4.3. Sensitive Information must not be transmitted over any communications medium from a portable computing device unless approved transmission encryption techniques are utilized.
- 4.4. Portable computing devices remotely connecting to university information resources from must do so utilizing approved transmission encryption techniques.
- 4.5. Unattended portable computing devices must be physically secure This means they must 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: Assistant Vice President for Technology

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

Office of Responsibility: Executive Vice President, Finance & Administration