The University of North Texas at Dallas Policy Manual	Chapter 14.000
14.003 Portable Computing	**Information Technology**

Policy Statement. It is the policy of the University of North Texas at Dallas to manage the University's information resources as strategic assets of the State of Texas. This policy provides specific guidance on the use of portable computing devices and their connection to the University's network. The policy also outlines responsibilities of information custodians to adequately protect data residing on portable devices.

Application of Policy. This policy applies to all University Users.

Definitions.

1. Information Resources. "Information Resources" means the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information of data and administered both centrally and within individual departments, on-campus and remotely, on a mainframe and network servers, and for use by single and multiple users.

2. Confidential Information. "Confidential Information" means information that is an exception from disclosure requirements under provisions of applicable state or federal law (e.g., Texas Public Information Act).

3. Portable Computing Devices. "Portable Computing Devices" means any easily transportable device that is capable of receiving or transmitting data to and from the information resources. These include, but are not limited to, notebook computers, handheld computers, Personal Digital Assistants (PDAs), pagers, cell phones, and smart phones.

4. Portable Storage Device. "Portable Storage Device" means an easily transportable device that stores electronic data. This includes, but is not limited to: flash/thumb drives, iPods, CD-Rs/CD-RWs, DVDs, and removable disk drives.

5. Remote Access. "Remote Access" means the act of using a computing device to access another computer/network from a location that is external to the primary facility or network (e.g., authentication mechanism, firewall, or encryption).

6. University Users. "University Users" mean all faculty, staff, students, contractors, volunteers, and individuals that maintain a business relationship with University that utilize mobile computing devices and connects to the University's network. Information resources may also be included in this category.

Procedures and Responsibilities

1. Only university-approved portable computing devices may be used to access the University's information resources. The Information Technology Department is responsible for determining the appropriate devices for the University.

   Responsible Party: Information Technology

2. Portable computing and storage devices, containing confidential information, shall be protected from unauthorized access as described in relevant university policies.

   Responsible Party: All University Users/Information Technology

3. Any confidential information stored on a portable computing or storage device shall be encrypted with an appropriate encryption technique, as determined by the Information Technology Department.

   Responsible Party: All University Users/Information Technology

4. All remote access (e.g., dial-in services, cable/DSL, modem, etc.) to confidential information from a portable computing device shall utilize encryption techniques, such as Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), or Secure Socket Layer (SSL).

   Responsible Party: All University Users/Information Technology

5. Confidential information shall not be transmitted via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions, such as Virtual Private Network (VPN), Wi-Fi Protected Access (WPA) or other secure encryption protocols are utilized.

   Responsible Party: All University Users/Information Technology

6. Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.

   Responsible Party: All University Users

7. Where appropriate, users must keep portable computing devices patched/updated and must install anti-virus software and a personal firewall.

   Responsible Party: All University Users/Information Technology

References and Cross-references.

Texas Government Code § 2054 – Information Resources

Texas Administrative Code, Chapter 202, Subchapter C and Department of Information Resources, Policy and Standards for Protecting Information Resources for Texas

University of North Texas at Dallas Information Resources Security Policy and Information Resources Acceptable Use Policy

Approved: 8/30/2010
Effective: 8/30/2010
Revised: