Purpose: The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at the <Company Name>.

Background/History: With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs at the <COMPANY NAME>. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at the <COMPANY NAME>.

Persons Affected: <COMPANY NAME> employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the <COMPANY NAME>.

Policy: It is the policy of the <COMPANY NAME> that mobile computing and storage devices containing or accessing the information resources at the <COMPANY NAME> must be approved prior to connecting to the information systems at the <COMPANY NAME>. This pertains to all devices connecting to the network at the <COMPANY NAME>, regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or <Organization Name> owned, that may connect to or access the information systems at the <COMPANY NAME>. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at the <COMPANY NAME> unless the media type has already been approved by the Desktop Standards Committee. The Desktop Standards Committee will maintain a list of approved mobile computing and storage devices.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the <COMPANY NAME>. These risks must be mitigated to acceptable levels.

Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive <COMPANY NAME> information must use encryption or equally strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the Data Resource Manager and Chief Information Security Officer, databases or portions thereof, which reside on the network at the <COMPANY NAME>, shall not be downloaded to mobile computing or storage devices.

Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall have knowledge of, sign, and adhere to the Computer Use and Information Security Policy Agreement (<COMPANY NAME> 350). Compliance with the Remote Access Standards, the Mobile Media Standards, and other applicable policies, procedures, and standards is mandatory.

Procedures:

Minimum Requirements:

- To report lost or stolen mobile computing and storage devices, call the Enterprise Help Desk at xxx-xxx-xxxx. For further procedures on lost or stolen handheld wireless devices, please see the *PDA Information and Procedures* section.
- The <COMPANY NAME> Desktop Standards Committee shall approve all new mobile computing and storage devices that may connect to information systems at the <COMPANY NAME>.
- Any non-departmental owned device that may connect to the <COMPANY NAME> network must first be approved by technical personnel such as those from the <COMPANY NAME> Desktop Support. Refer to the Mobile Media Standards for detailed information.
- Submit requests for an exception to this policy to the Information Protection Services Office via the Policy Exception Request form (EXEC 205).

Roles and Responsibilities:

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the <COMPANY NAME> and they must annually complete the <COMPANY NAME> 350. Before connecting a mobile computing or storage device to the network at <COMPANY NAME>, users must ensure it is on the list of approved devices issued by the ISD.

The **Enterprise Help Desk** must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The **Information Protection Services Office** is responsible for the mobile device policy at the <COMPANY NAME> and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by the <COMPANY NAME>.

The **Information Systems Division** is responsible for developing procedures for implementing this policy. The Desktop Standards Committee will maintain a list of approved mobile computing and storage devices and will make the list available on the intranet.

Definitions:

CD: A *compact disc* (sometimes spelled *disk)* is a small, portable, round medium made of molded polymer (close in size to the floppy disc) for electronically recording, storing, and playing back audio, video, text, and other information in digital form.

DVD: The *digital versatile disc* stores much more than a CD and is used for playing back or recording movies. The audio quality on a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.

Flash Drive: A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as a keychain drive, USB drive, or disk-on-key. A keychain drive, which looks very much like an ordinary highlighter marker pen, can be used in place of a floppy disk, Zip drive disk, or CD.

Handheld wireless device: A communication device small enough to be carried in the hand or pocket and is also known as a Personal Digital Assistant (PDA). Various brands are available, and each performs some similar or some distinct functions. It can provide access to other internet services, can be centrally managed via a server, and can be configured for use as a phone or pager. In addition, it can include software for transferring files and for maintaining a built-in address book and personal schedule.

Media Type: For the purpose of this policy, the term "media type" is interchangeable with "mobile device." Not to be confused with media makes, models, or brands.

Media Type Model: Refers to the brand of media device such as Sony, Treo, or IBM.

Mobile Devices: Mobile media devices include, but are not limited to: PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

Modems: A device that modulates and demodulates information so that two computers can communicate over a phone line, cable line, or wireless connection. The connection talks to the modem, which connects to another modem that in turn talks to the computer on its side of the connection. The two modems talk back and forth until the two computers have no further need of either modem's translation services.

PDA: The *Personal Digital Assistant* is also known as a handheld. It is any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information handy. Many people use the name of one of the popular PDA products as a generic term, such as Hewlett-Packard's Palmtop and 3Com's PalmPilot.

Plug-In: Programs that can easily be installed and used as part of your Web browser. A plug-in application is recognized automatically by the browser, and its function is integrated into the main HTML file that is being presented. Among popular plug-ins is Adobe's Acrobat, a document presentation and navigation program that provides a view of documents just as they look in the print medium. There are hundreds of plug-in devices.

Wireless Networking Cards: Mobile device for wireless internet connectivity from a laptop. This card allows mobile users the ability to access a secured connection to the internet via a specified vendor.