Remote Access Mobile Computing Storage Policy

Last Update Status: *Retired*

1. Overview

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>.

2. 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>.

3. Scope

<Company Name> employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the <Company Name>.

4. Policy

4.1 General 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.

4.2 Procedures

To report lost or stolen mobile computing and storage devices, call the Enterprise Help Desk. For further procedures on lost or stolen handheld wireless devices, please see the 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.

4.3 Roles & 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>. 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 Infosec Team 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 (ISD) 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.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Flash Drive
- Mobile Device
- Plug-in

8 Revision History

Date of Change	Responsible	Summary of Change
July 2014	SANS Policy Team	Converted to new format and retired. Relevant sections added to new Trusted Device Policy.