Security of Mobile Computing Devices

SUBJECT: Security of Mobile Computing Devices

SOURCE: Office of the Dean, IU School of Medicine

POLICY NO: IUSM SEC-05

DATE ISSUED: 18 Nov 04

SCOPE:

This policy applies to all faculty, learners, and staff of the IUSM, as well as vendors, contractors, partners, collaborators, and any others doing business or research with the IUSM. Any other parties, who use, work on, or provide services involving IUSM computers, technology systems, and/or data will also be subject to the provisions of this policy.

IUSM computing resources have been developed to encourage appropriate widespread access and distribution of data and information for the purpose of accomplishing the educational, clinical, and research missions of the school. This policy will not supersede any Indiana University policies but may introduce more stringent requirements than the university policy.

POLICY STATEMENT:

1. Any mobile computing device, including personally-owned devices, accessing IU data is subject to all IU and IUSM policies. If the capability exists, all mobile computing devices will be configured to:
   o receive periodic security updates from the operating system vendor,
   o have anti-virus software enabled, active, and up-to-date,
   o have encryption enabled and active
   o have an application-level firewall installed and active

REASON FOR POLICY:

The purpose of this policy is to protect the confidentiality, availability, and integrity of Indiana University School of Medicine (IUSM) and partner data while it is stored, transmitted, viewed, or used on mobile computing devices. The protection of IU data is paramount and this policy applies to all mobile devices used to access any university data or system.
DEFINITIONS:

*Mobile Computing Devices* are any type of device that is capable of collecting, storing, transmitting, or viewing electronic data or images and may not have a wired connection to the network. This includes (but is not limited to) laptops, tablets, smartphones, and portable storage devices.

SANCTIONS:

If it is suspected that this policy is not being followed, report the incident to the Departmental IT manager or representative and the IUSM Chief Information Security Officer.

Any exceptions to this policy must be approved in advance by both the IUSM Chief Information Security Officer and the IUSM Chief Information Officer.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Indiana University Policy IT-02, *Policy on Sanctions for Misuse or Abuse of Indiana University Technology Resources*.

HISTORY:

1. IUSM SEC-05, 30 Dec 05, first draft of policy
2. Policy reviewed on February 24, 2011
3. Sections headers updated August 6, 2013