Mobile Device Security Standards

Background

In February 2013, IU passed the Mobile Device Security Standard, Policy IT-12.1. This policy sets minimum standards for encryption and other security measures intended to protect data on mobile devices such as laptops, tablets, and phones. Compliance with this policy is required for any device used to “access, store, or manipulate institutional data”. For example, if you use your mobile device to access your IU email, then you are subject to these security requirements. Furthermore, mobile devices used to access critical data are subject to additional safeguards.

This document is intended to give a summary of the SoIC recommended steps to secure popular devices in use by our Faculty, Staff, and Students. If you have any questions about the IU policy or the steps needed to be in compliance, please see the IT Policy: Mobile Device Security or Contact Us.

Reference: How can I protect data on my mobile device?

Windows Laptop

- If your Windows laptop is encrypted with Microsoft Bitlocker, you should see a blue screen at startup requesting your Bitlocker unlock pin. If your Windows laptop is encrypted with PGP Whole Disk Encryption you will see a gray and white PGP Desktop login screen upon boot up. Also see: https://kb.iu.edu/d/bavx

1. Encrypt your computer as described in the Microsoft document Turn on Bitlocker Device Encryption. Be sure to enable TPM options in your computer’s BIOS. Set your computer to request a Bitlocker pin by setting that option in Control Panel, Bitlocker Encryption, Set Bitlocker Startup Preferences, Require a pin at every startup. Be sure to backup your encryption key. You may also use Symantec PGP to encrypt your laptop as directed here: https://kb.iu.edu/d/azmz
2. To be compliant with the IU policy, you must select a password that meets the IU Password and Passphrase Guidelines
3. The system must auto-lock after no more than 15 minutes of inactivity.

Mac OS X Laptop

- To verify that your Mac is encrypted with FileVault, go to System Preferences/Security & Privacy and click on the FileVault tab.

1. Encrypt your computer using FileVault 2
2. To be compliant with the IU policy, you must select a password that meets the IU Password and Passphrase Guidelines
3. The system must auto-lock after no more than 15 minutes of inactivity.
4. Register your device in the Device Enrollment Program (DEP) per Securing your Apple Macintosh Laptop For Use at Indiana University

IOS Devices (iPhones, iPads, and iPods)

- Even if you do nothing else, just setting a 6+ character passcode can get your IOS device in compliance with IU policy

1. Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). You enable it by simply enabling a passcode. You can also use a product such as Symantec Mobile Encryption for iOS, available via the iTunes Store.
2. Set a device passcode per the KB document How can I secure my iPhone, iPad, or iPod touch?
3. For added security, we strongly recommend you register your device per Securing Your iPad For Use at Indiana University. Registration is required for all SoIC-owned ipads.
4. For personally-owned devices, owners may choose to use the auto-erase after 10 failed login attempt feature or the remote wipe feature offered by Find my iPhone/Find my iPad/Find my Mac service.

Android Devices

- Even if you do nothing else, just setting a 6+ character passcode can get your android device in compliance with IU policy

1. Secure the device per the KB document How can I secure my Android OS device?
2. You can use the Android Device Manager to locate, ring, and wipe your phone. In order to enable the remote wipe feature (which we strongly recommend), you will need to open the “Google Settings” app, select “Android Device Manager”, and enable “Allow remote factory reset”.

Linux Laptop
1. Full disk encryption is available as an option when installing many Linux distributions, including Ubuntu (version 12.10 and later) and Fedora (version 14 and later). You should select a linux distribution that supports full disk encryption and not just encrypt your home folder since sensitive information can be written in locations outside of your home folder. For Ubuntu, you just need to check "Encrypt the new Ubuntu installation for security" option on the "Installation Type" screen during the OS install. For Fedora, you will just need to enable LUKS (Linux Unified Key Setup) during the installation and there is more detailed information in the Fedora disk encryption guide. If you have already installed the operating system without full disk encryption you are advised to back up your data and reinstall.

2. You must select a password that meets the IU Password and Passphrase Guidelines

3. By default, most linux distributions will enable screen locking after some period of inactivity. To be compliant with the IU policy, the system must auto-lock after no more than 15 minutes of inactivity.

Other Devices

Any device type not specifically listed here is still subject to the requirements of IT-12.1 Mobile Device Security.