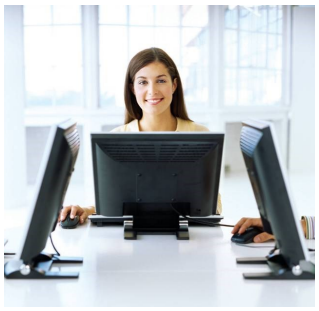
Laptop/Mobile Device Requirements



IU has a new policy (IT-12.1) which outlines security requirements for laptops and other mobile devices. The policy can be reviewed at https://protect.iu.edu/online-safety/policies/it121.html

All systems and mobile devices, including devices that are personally owned, must comply with IU requirements in order to be used for university business.

Table of Required Safeguards by Device Type

Mobile	Passcode/Passphrase	Intrusion Prevention	Encryption	Remote Wiping
Handheld mobile device (i.e. Smart Phone, Tablet, etc.)	Required – minimum 4-character passcode using at least 2 unique characters, and auto lock after a maximum of 15 minutes of inactivity.	Required - Lockout or wipe after 10 incorrect attempts, OR Increasing delay after incorrect attempts.	Recommended in all cases if supported by the device. Required for all intended use involving critical information. [2]	UIPO Incident Response or the Support Center will assist with remote wiping based on the circumstances of reported loss or theft.
Laptop/Notebook Computer	Required – Passphrase meeting IU requirements [3] must be used when device boots, and auto lock after a maximum of 15 minutes of unattended inactivity.	Required – lockout after 25 incorrect attempts within 2 hrs.	Required - full disk.	Not applicable

[2] Remember that use of mobile devices to access, store, manipulate critical information requires written approval from a senior executive of the unit or the IRB and encryption on the device and in transit.

[3] See KB article on Passwords and Passphrases: https://kb.iu.edu/data/acpu.html

Required Actions

- Use a **whole-disk encryption** program on all laptops and mobile devices. For more information: http://kb.iu.edu/data/bcnh.html#laptop
- Maintain all software and mobile devices with the latest vendor recommended updates. Note: PCs must have Windows 7.x or later since earlier versions such as Windows XP do not have the necessary safeguards in place. IU recommends Secunia PSI for software updates. For more information: http://kb.iu.edu/data/azfj.html
- Run **anti-virus software**. For more information: http://kb.iu.edu/data/aggp.html
- Use **Virtual Private Network (VPN)** or login through IUanyWare when working remotely. For more details, please review the kb articles referenced on the left.
- Do not store critical data on personal storage mediums such as flash drives, disks or local drives.

LOGGING IN FROM OFF-CAMPUS?

You must use **VPN** prior to accessing institutional data via the network or IU systems (e.g., IUIE, CBI, SIS, etc…).

Instructions for Laptops/Desktops

http://kb.iu.edu/data/aygt.html

Instructions for iOS

http://kb.iu.edu/data/batd.html

Instructions for Android Devices

http://kb.iu.edu/data/bcin.html

REASONS FOR VPN

- ◊ Allows you to protect the information you're transmitting over the Internet by encrypting all traffic between you and IU
- ◊ Allows you to act as part of IU's network when you're off campus

IUanyWare

Another option available for logging in off campus is the Remote Desktop application in IUanyWare. Instructions for setup of IUanyWare can be found at: https://kb.iu.edu/data/bbbu.html

***For questions regarding laptop and mobile device requirements you may contact your LSP.**

Revised 9/2015