1610 GD.02 Device Security Guidelines

Revision Date: *May 17, 2016*

Overview

These device security guidelines are recommended for all University desktops, laptops, workstations, and tablets (which run a desktop class operating system).

Device Configuration Guidelines

Note: ITS services are recommended to meet the following guidelines: encryption, patching, anti-virus protection, and backup. Please contact the Helpdesk 203-432-9000 for more information on these services.

1. *Encryption* – Whole disk encryption is not only recommended but also encouraged for all systems that conduct Yale business. All external storage used to transport Yale data should be encrypted.
    a. *Windows* – Windows devices should be capable of running BitLocker. Devices that subscribe to the ITS-managed Bitlocker encryption service require a Trusted Platform Module (TPM) chip.
    b. *Apple* – Apple devices should be capable of running FileVault 2.
        i. It is recommended that Apple systems are not configured to dual-boot (including the use of Boot Camp). If there is a need to run a Windows operating system within Mac OS X it is recommended that Windows be installed in a virtual machine (VM).
    c. *Linux* – Linux devices should be capable of running LUKS.
2. *Administrator Privileges* – User Access Control (UAC) should be enabled on administrator accounts.
3. *Registration* – All devices should be registered in the Yale IP Address Management System (Proteus).
4. *Network Address* – Private IP addresses should be used on all devices such as computers, laptops, printers, research devices, etc.
5. *Identification* – All devices should employ IBM Endpoint Manager (BigFix) for identification purposes.
6. *Operating System* – Systems should be in compliance with the published Yale Standard Supported Operating Systems.
7. *Patching* – All devices must be fully updated and patched. Questions or concerns regarding up-to-date device patching can be directed to scanit@yale.edu.
8. *Anti-Virus Protection* – Installation and automatic update of anti-virus/anti-spyware software (the ITS-managed IBM Big Fix AV is recommended).
9. *Enterprise Directory and Authentication* – Devices should be on the Yale domain and all system logon requests should be done through Yale credentials and will be processed through Yale's enterprise directory.
10. *Backup* – All devices should be backed up (the ITS Crashplan backup service is recommended). Backups should be completed on a regular interval.

11. *Inactivity Lock* – Automatic locking and password protection of systems after 15 minutes of inactivity should be enabled.
12. *Application Security* – Applications that increase the vulnerability of systems, including, but not limited to the following, should be removed:
    a. Peer to Peer (P2P) file sharing
    b. Any application which is illegal or against Yale policy
    c. Hacking utilities (e.g. password recovery programs, spyware, keystroke loggers)
    d. Adware (or advertising-supported software)
    e. Copyright software that has not been acquired in accordance with Yale's procurement guidelines as well as the vendor's copyright agreement.
    f. TOR
    g. Proxy software and third-party VPN clients for non-business purposes
13. *Software* – All software being considered for installation should be vetted by Information Security prior to installation.
14. *External Messaging Applications* – Yale business should be conducted only on Yale-approved instant messaging applications.
15. *Procurement* – All new desktop and laptop systems should be purchased according to the "Recommended Computing Devices" guide (http://its.yale.edu/software-technology/buying-guide/recommended-computing-devices). Please consult with your local IT support provider prior to purchasing any device.