Workstation Security Standards Summary

from: http://www.buffalo.edu/ubit/policies/guidance-documents.html

Standards for Low Risk Data (Category 3 -public)

2.1 Security Patching
2.2 Password Authentication
2.3 Malware Protection
2.4 Supported Operating Systems
2.5 Supported Software
2.6 Firewall
2.7 Run as User
    2.7.1 Administrative Account Privileges for End Users
2.8 Whole Disk Encryption

Standards for Moderate Risk Data (Category 2 -private)

Note: Incorporates all standards listed for Low Risk Data, plus:

2.9 Scan for Personally Identifiable Information (PII)
2.10 Inventory
2.11 Inactivity Timeout
2.12 Hard Drive and Printer Sharing
2.13 Login Banner
2.14 Dispose/Re-use
    2.14.1 Disposal
    2.14.2 Re-use
2.15 Remote Desktop Access

Standards for High Risk Data (Category 1 -restricted)

Note: Incorporates all standards listed for Low Risk Data and Moderate Risk Data, plus:

2.16 Application Whitelisting
2.17 Account Lockout
2.18 Vulnerability Scanning
2.19 Physical Security
2.20 Security Benchmarking

3. Mobile Device Standards

3.1 PIN or Passcode
3.2 Inactivity Timeout
3.3 Encryption
3.4 Remote Location and Erase
3.5 Disposal/Re-use
3.6 DO NOT Store Category 1-Restricted Data

5. Personally Owned Devices

5.1 Standards for Low Risk Data The minimum standards for desktop, laptop, mobile devices, and other endpoint devices identified in this document apply to personally owned devices, commonly referred to as Bring Your Own Device (BYOD), that (1) can access university data, (2) contain locally stored university data, (3) process university data, and/or (4) access the university network.

5.2 Standards for Moderate Risk Data and High Risk Data In order to access moderate risk data and/or high risk data (including Category 1Restricted Data) on a personally owned desktop, laptop, or other mobile device, additional standards apply. Users are required to contact a system administrator for details.

Recommendations from the ISO for Home and Personal Devices:

Many of these standards or controls above are the same things you should do at home with your home computer! These are normal, good practices for home use:

2.1 Security Patching (auto-updates)
2.2 Password Authentication (login required to use the computer, not just turn it on)
2.3 Malware Protection (free or paid anti-virus)
2.4 Supported Operating Systems (if connecting to the network/Internet)
2.6 Firewall (local to the machine and on your cable modem-ISP router ("edge router"))
2.7 Run as User (create two IDs -one for you, one when needing admin)
2.8 Whole Disk Encryption (BitLocker, FileVault -don't lose that password!)
2.11 Inactivity Timeout (screen saver with password)
2.12 Hard Drive and Printer Sharing (disable unless needed)
2.14 Disposal (wipe or remove drives or "shred"/destroy them before disposal)
2.15 Remote Desktop Access (only if you need it for personal use, and then secure it well!)
2.19 Physical Security (lock your house doors and windows! Don't leave laptops in the car.)