Policy 5.10 Requirements

Draft - 05.06.16.01

If your computer is NOT managed by CNF IT, then you are personally responsible for meeting the requirements of Cornell Policy 5.10 (as well as other applicable IT policies). CNF IT can assist you in meeting the requirements.

Included is a copy of the CNF Cybersecurity Policy, which links to relevant Cornell IT policies.

Tool Control Computers will be exceptions to the below policy requirements. The Unit Security Liason will maintain a list of all computers which are exceptions. CNF will need to submit such an inventory to the Unit Security Liason.

Any other exceptions to the below policy requirements must be documented and submitted to the Unit Security Liason.

Confidential Data Requirements

CNF does not handle data Cornell considers as Confidential Data, so we will not worry about those requirements. Confidential Data is any of the following when in appearance with an individual's name or other identifier:

- Social Security Numbers
- Credit Card Numbers
- Driver's License Numbers
- Bank Account Numbers
- Protected Health Information as defined under HIPPA

Confidential data must not be stored on or processed by CNF servers (including email) or workstations.

Baseline Requirements for all Cornell owned Devices

- Must not leave the country - additional requirements.
- Non CUSoftware programs - oss, foss, or commercial - must be ok'ed or undergo Security Assessment by ITSO
- Register the computer on the network via https://mycomputers.cit.cornell.edu
- Computer's OS must be kept up to date
  - No later than 14 days after release of patches
- All software installed on the computer must be kept up to date
  - No later than 14 days after release of patches
- Consistent or regular use of any account with administrative privileges is inappropriate.
- All accounts must have strong passwords at least equivalent to the requirement for NetID passwords
- Run AntiVirus and Firewall software
  - Both are now built into Windows
  - MacOS X includes a built in Firewall
  - Linux includes a built in Firewall
- Configure the screen saver so the system password is needed to unlock the screen after the computer has been idle for 15 minutes, or less

Additional Requirements for Desktop and Laptops

- Whole Disk Encryption must protect all local, persistent storage (eg hard disk) when the system is powered off.
  - Does not apply to VMs, if the hosting disk is already encrypted
  - Keys must be centrally escrowed.
    - Recommendation: Escrow in Password Manager Pro central IT service: http://www.it.cornell.edu/services/password_escrow/
- File shares and other mechanisms for file access must be password protected - no open shares, public folders, or drop folders are permitted on individual systems.
- No shared or passwordless logins.