

Baseline IT Security Requirements

Version 1.0 – 01 Nov 07

To better safeguard the university's data and IT resources, the IT Security Office requires the following practices. These requirements apply to any system that is (a) used to conduct university business or (b) connected to Cornell campus networks.

Here, and elsewhere, “university business” does *not* include viewing or updating your individual university data.

These requirements, as well as the accompanying requirements for securing Confidential Data, reflect an approach referred to as “layered defense” or “defense-in-depth.” We need to build defenses on multiple levels — network, system, application, data — so that if the integrity of one is weakened, another may still be able to provide sufficient protection. It is the sum of all these measures, and not reliance on any particular aspect of security, that will move the university towards a more secure IT environment.

Items labeled as a *Suggestion* reflect a beneficial practice that might be a requirement at some future date.

A. Exceptions

For all computers or other IT resources that are not able to meet these security requirements, the following exception process must be followed:

1. IT resources that cannot meet the following requirements must be identified to the appropriate Unit Security Liaison. The Unit Security Liaison will look for alternate methods to address the risk that is being addressed. If an alternate security solution can be found to address the specific risk, an exception is not required.
2. The Unit Security Liaison may determine a local solution or consult with the IT Security Office for assistance
3. The Unit Security Liaison will maintain a list of all IT resources that require an exception and review them on an annual basis.

B. All Computers

1. Keep all operating system, server and application software up-to-date.
 - A local patch management process must ensure that all security /critical updates are installed as soon as possible, and no later than five business days after their release.
2. Configure user privileges to be as low as possible while still meeting business needs. Consistent or regular use of the Administrator or root account is not recommended.
3. Ensure all accounts have strong passwords at least equivalent to the strength required for NetID passwords.
 - No electronic distribution of passwords in the clear, i.e. transmission must be encrypted.

4. For any computer system that is not in a secure, private space, run a password-protected screen saver, or some other console-locking mechanism, that is triggered after fifteen minutes (or less) of inactivity.
5. Ensure local / personal firewalls (Symantec Client Firewall, Windows Firewall, MacOS X firewall, etc.) and / or IPSec filters are installed and running.
6. Where applicable, run anti-virus and anti-spyware software with daily updates and active protection enabled.

C. Specific to Desktops and Laptops

1. Local file shares cannot be configured as open shares; all shares must be password protected.
Suggestion: Use a departmental file server instead of local shares.
2. If multiple individuals use a system, each should have their own login account, or the system should be rebuilt prior to each individual use. This also applies to “loaner” systems.

D. Specific to Application and File Servers

1. Follow hardening guidelines for the operating system and any applications or services that connect to the network.
 - Along with the software vendor, credible sources for guidelines include NIST, CIS, NSA, SANS, FIRST.
 - Disable all network services, including specific application features, that are not needed for the system to fulfill its function.
 - Change any passwords with default values set by the vendor.
2. No shared usernames and passwords.
 - Where shared accounts *are* necessary, maintain a local inventory of who has access to the account.
 - Change the password for any shared account when there is any change in personnel or access requirements.

E. Specific to Public Workstations and Kiosks

Note that point (4) under All Computers about console locking does not apply to this type of system.

Note that these requirements do not apply to computer labs and similar environments with systems that are not for use by the general campus population and require a unique, individual login.

1. Such systems may not be on the same subnet as computers used to conduct university business.
2. Such systems must display an appropriate logon banner or bear signage with:
 - a statement about responsible use;
 - a warning about using the system for personal or sensitive data; and
 - a reminder to logout and / or clear any active credentials.

3. No local file shares permitted.
4. If system privileges are required for users (users can write files to the computer), then a full system rebuild must occur prior to each individual use.
5. Visually inspect such systems regularly, at the very least on a quarterly basis, to see if physical security has been compromised.

F. Network Security

1. Use Edge ACLs or a local network firewall to implement packet filtering on staff networks and networks with servers used for administrative business.
 - The primary goal is to limit network access to servers and other critical resources. Consider to what extent you might want to also filter traffic to and from individual computers.
 - When designing a rule set, make sure you thoroughly understand the services required for a given network, taking into account the needs of your department and of others who might use it. CIT's Security Engineering group can assist you in developing a rule set.
 - IPSec, a host firewall and similar measures can be used to supplement network ACL/firewall rules.
2. All systems must be registered by MAC address and assigned to a user or network administrator, including any departmental wireless networks and wireless access points. No unregistered systems should be on any Cornell network. (This requirement is detailed in University Policy 5.7, Network Registry.)

Suggestion: Any university business conducted on a wireless connection should use Red Rover-Secure, or a departmental wireless network with equivalent or stronger security. (This will become a requirement once it reasonable to assume that older staff laptops that don't work with Red Rover-Secure have been replaced.)

G. Reviews and Assessments

The department is responsible, on at least on an annual basis, for assessing the local infrastructure and environment. This assessment should follow the IT Security Office's security assessment methodology and include:

1. Review edge ACLs and other network security mechanisms.
2. Run a vulnerability scanner, such as Nessus or GFI LANguard, on all unit subnets and remediate high-risk vulnerabilities.
3. Review all file and application servers, including checking for vulnerabilities in web sites, databases, etc., and – as appropriate -- scanning for Confidential data.
4. For a sample set of staff computers conduct content inventories using Spider or comparable application to ensure no improper instances of Confidential data.

Suggestion: Run an annual, or more frequent, content scan of all systems.

5. Audit account distribution to ensure that only current, authorized personnel have access to departmental systems.