

BTI Computer Security Policy

Due to the increased number of compromised systems at BTI a Computer Security Policy will be implemented and enforced to help secure systems and minimize system down time. This policy is not intended to be punitive in nature, but rather is a means of safeguarding your computer system and those of your colleagues.

The goal of this policy is to prevent:

- Propagation of viruses
 - Unauthorized access to systems (hacked systems)
 - Theft of bandwidth (hacked systems serving games, videos, etc)
 - Lost or altered data on compromised systems
 - System down time due to infected, damaged systems
-

Computer Support Staff will assist all BTI computer users to assure that machines are set up in the most secure manner (configuring LiveUpdate, running Windows Update, performing NAV scans). Please contact Joan Curtiss or Elaine Van Etten at btihelp-1@cornell.edu to schedule an appointment.

Consequences for failing to adhere to this policy are indicated at the end of this document.

In order to provide the best possible protection for your machines, the following guidelines must be followed by all BTI computer users.

All PC/Windows users at BTI will

1. Have a secure Windows password for ALL system accounts.

A secure password must meet the following complexity requirements:

- Minimum of 6 characters
- Must contain at least one letter and one number
- Must not be a word found in ANY dictionary
- Must not be a name, birthday, or other easily obtained information
- Must be changed at least every 90 days

This means that when Windows starts you MUST enter a password. If you can "Cancel", hit the Enter key to bypass, or if you are not prompted for a password on startup, then your system can easily be accessed by anyone on the network!

2. Run Norton Antivirus Realtime protection and routinely scan drives for viruses.

-Norton Realtime protection **must** be enabled. (Realtime protection automatically scans and detects infected files when copying, executing, saving, or opening infected files from networked sources such as email and mapped network drives)

This can be verified by clicking on the NAV icon (gold shield) in the lower right corner of the screen and confirming the check mark by "Enable Realtime Protection".

-All hard drives must be manually scanned for viruses on a weekly basis.

Start NAV -> choose Scan computer -> Select drives to scan

-You also have the capability to schedule automatic daily or weekly scans but you must verify that these scans are being performed as scheduled

3. Manually run Norton LiveUpdate on a weekly basis or whenever virus notices are sent.

-Start NAV -> Click LiveUpdate

-You also have the capability to schedule daily or weekly LiveUpdates but you must verify that these scans are being performed as scheduled

4. Scan for and install critical Windows updates and service packs as they become available.

-Critical updates often repair known software bugs and patch system vulnerabilities that allow unauthorized access to systems. It is imperative that these fixes be installed as soon as they become available.

In general follow the path: Start Menu -> Windows Updates -> Scan for updates -> Install

Windows Update can also be configured to automatically download available updates. **It is still necessary to routinely perform a manual scan for updates** since Service Packs are not downloaded through this service and there have been instances when Windows Updates failed to download the most current releases.

5. Take suggested preventive or corrective measures announced by BTI computer support personnel as they become known to the computing community and do so in a timely manner.

All Mac OS X users at BTI will

1. Have a secure log on password for ALL system accounts.

A secure password must meet the following complexity requirements:

-Minimum of 6 characters

-Must contain at least one letter and one number

-Must not be a word found in ANY dictionary

-Must not be a name, birthday, or other easily obtained information

-Must be changed at least every 90 days

This means that when the system boots you MUST enter a password. If you can "Cancel", hit the Enter key to bypass, or if you are not prompted for a password on startup, then your system is at risk of being compromised.

2. Run Norton Antivirus Realtime protection and routinely scan drives for viruses.

-Norton Realtime protection **must** be enabled. (Realtime protection automatically scans and detects infected files when copying, executing, saving, or opening infected files from networked sources such as email and mapped network drives)

This can be verified by starting NAV and confirming the check mark by "Enable Realtime Protection".

-All hard drives must be manually scanned for viruses on a weekly basis.

-Start NAV -> choose Scan computer -> Select drives to scan

-You also have the capability to schedule automatic daily or weekly scans but you must verify that these scans are being performed as scheduled

3. Run Norton LiveUpdate on a weekly basis or whenever virus notices are sent.

-Start NAV -> Click LiveUpdate

-You also have the capability to schedule daily or weekly LiveUpdates but you must verify that these scans are being performed as scheduled

4. Use Software Update to check for updates to software.

5. Take suggested preventive or corrective measures announced by BTI computer support personnel as they become known to the computing community and do so in a timely manner.

All other Mac OS users (OS 9.x and 8.x)

1. Run Norton Antivirus Realtime protection and routinely scan drives for viruses.

-Norton Realtime protection **must** be enabled. (Realtime protection automatically scans and detects infected files when copying, executing, saving, or opening infected files from networked sources such as email and mapped network drives)

This can be verified by starting NAV and confirming the check mark by "Enable Realtime Protection".

-All hard drives must manually be scanned for viruses on a weekly basis.

Start NAV -> choose Scan computer -> Select drives to scan

-You also have the capability to schedule automatic daily or weekly scans but you must verify that these scans are being performed as scheduled

2. Run Norton LiveUpdate on a weekly basis or whenever virus notices are sent.

-Start NAV -> Click LiveUpdate

-You also have the capability to schedule daily or weekly LiveUpdates but you must verify that these scans are being performed as scheduled

3. Take suggested preventive or corrective measures announced by BTI computer support personnel as they become known to the computing community and do so in a timely manner.

BTI's network will be routinely scanned and the following actions will be taken when vulnerable systems are found:

1. External internet access will be blocked for any systems posing a serious threat to BTI's network security.

(External access is network access to off-campus locations such as remote servers and web sites. Users will still be able to connect to BTI printers and other **local** systems.)

This will be automatic when notices are received from Cornell's Network Operations Center (NOC) regarding BTI systems propagating viruses or serving illegal material (movies, games, etc).

This will also be automatic on all systems that have blank system passwords (Windows Users)

2. Those systems that are not kept current with Norton Antivirus virus definitions and Windows Critical Updates may also have all internet access blocked until the situation can be resolved.

Users must follow the Computer Security Policy or network access may be denied.

3. Users will be notified of potential security risks and will be given time to investigate and remedy any vulnerabilities.

-An example may be a system with Guest accounts enabled or passwords that don't expire.