

Christopher Newport University Security Initiative 2007

As the University has grown in size and complexity, so must the measures we take to ensure the security of our institutional data and our information technology resources. Therefore, the University Technology Committee (UTC)* has adopted the following policies, effective July 1, 2007:

1. Password Management.

Passwords must:

- contain at least eight (8) characters;
- be a combination within the first eight positions of **all** of the following—upper case letters, lower case letters, numbers, and special characters [e.g. !@#];
- be changed at least every 90 days;
- passwords may not be reused.

What this means to you: Within the next three months Windows users will be prompted to change their passwords to comply with these standards. Your new password must follow the rules above. That new password will be good for 90 days, and when it is time to select a new password your computer will prompt you to do so.

Mac users will also need to comply with these requirements. At first, Mac users will change their computer passwords manually every 90 days; later, however, automatic reminders will be sent.

Similar security password management policy will be implemented for MyCNU in the fall of 2007. More details will be released at that time.

2. Physical Access (screen locking).

A screen lock must be active on all computers and other devices used for data access--when they are not in use or not in personal custody. In order to help faculty and staff comply with the Commonwealth's standard,

- ITS will remotely implement a screen lock on most devices on the CNU network.

Users of devices that cannot be protected by the automatic ITS lock are responsible for activating an equivalent system.

What this means to you: If you have not used your computer for 15 minutes, a login screen will automatically appear on your display. Your computer is locked, although you have not been logged out of any system. You must enter your password to regain access to your computer.

3. Non-University Owned Devices Attached to the CNU Network

Network devices that are owned personally by faculty, staff, or students, including laptops, desktops, and network printers, are subject to the same security requirements as University-owned machines on the network.

• For computers, an up-to-date operating system and anti-virus program are required. Verification of satisfaction of these requirements must be done by IT Services before these privately-owned devices are connected to the CNU production network.

What this means to you: If you plan to attach your personal laptop to the CNU network by means of a hard-wired connection, you need to take your computer to the Helpdesk in

McMurrin Hall so that IT Services can verify that your laptop is fully patched, virus free, and virus protected.

* UTC Membership: Chief of Staff; Executive Vice President for Administration and Finance; Vice Provost; Vice President of Student Services; Internal Auditor

4. Removal of Person-Identifiable Information from Campus (Data Transport)

In order to safeguard the information stored and used on mobile computing units such as laptops, PDAs, portable hard drives and flash drives, individuals who transport University person-identifiable information off campus must have the written permission of the UTC, and must protect the data by encryption and passwords.

Person-identifiable information includes any FERPA and HIPPA data such as the following:

- Social Security Number

- Driver's license number

- Student identification number (ID#)

- Bank account numbers

- Credit or debit card numbers

- Other banking information in combination with any required security code, access code, or password that would permit access to an individual's financial account.

IT Services recommends the alternative and more secure approach, where possible, of using the University's virtual private network (VPN) connection over the Internet so that users can connect to their work computers from home.

What this means to you: If you must take data in an electronic or printed state containing any of this information off campus, you must get permission from the UTC. If the data is in an electronic format, the data must be in a device that is password protected. It must be transported from and to campus in an encrypted USB drive or its equivalent. If you use a VPN, which allows you to remotely log into your work computers securely from off-campus over the internet, you will satisfy this data transport policy.

5. Local Administrator Rights

In order to comply with the Commonwealth's requirement to allow the use only of Agency approved software on University systems, all software must be installed on University systems by IT Services or its designee. Accordingly, all presently-active local administrative rights held by individuals will expire on June 30, 2007.

Instructional faculty in their educational and research activities are exempt from Policy 5 and for these activities may be granted local administrator rights.

Any other exceptions to the policy must be approved by the UTC in response to a written request submitted by the individual desiring local administrator rights and through the requester's department head. Persons for whom having local administrator rights is critical to the satisfactory performance of their duties are encouraged to apply for an exception in a timely manner. Department heads of persons to whom exceptions have been granted must maintain documentation that any software installed by these persons is legally licensed and must assure continued compliance with licensing requirements by a periodic audit, the results of which are submitted to the UTC.

What this means to you: If you need software loaded onto your individual University computers, you must place a request with the Helpdesk in McMurrin Hall. For standard software on hand, the Helpdesk will complete the request within two business days. Special procedures apply to laboratory computers.