Cleveland State University

University Computer Hardware Policy

Desktop / Notebook / Tablet Computers

1. All PCs (Desktop, Notebook, or Tablet) must be purchased according to the University PC Procurement process.

2. Every PC will run University-approved antivirus software and its auto updating agent, if available.

3. Every PC will run University-approved remote management software that is enabled.

4. Every PC will run a current vendor-supported operating system that is updated at the regular vendor-defined cycle, except as otherwise directed by IS&T.

5. The removal of PC management, antivirus, network or security software is not allowed. Audits of systems will be performed periodically to ensure all systems are kept current

6. The audits will filter findings and then present them to the appropriate support staff for remediation.

7. Every effort will be made to prevent audits from causing operational failures or disruptions.

8. Because not everyone is technically knowledgeable to ensure that computers are properly maintained, automatic processes and/or computer technicians may be dispatched to perform these updates. The IS&T Call Center at x5050 should be contacted for assistance for any computer-related issues.

9. All PCs must be disposed of according to the University Policy for Secure Disposal of Computers and Digital Media

Audit/Risk Assessment via Vulnerability Scans

1. Network security scanning will be performed by the IS&T Security Department of Cleveland State University. The IS&T Security Department will utilize software as it best sees fit to perform electronic scans on all network attached devices owned or operated by Cleveland State University. This policy also covers any computer and communications devices that are on Cleveland State University's network, but which may not be owned or operated by CSU. For example, this will include but is not limited to all machines on the wireless network (WoWnet), dial-in network, vendor hardware, and any personal machines that are brought into the University and plugged into a network port.

2. Vulnerability Scans will be conducted to:
   - Ensure integrity, confidentiality and availability of information and resources
   - Ensure machines are patched against the latest vulnerabilities
   - Ensure conformance to Cleveland State University security policies
   - Investigate possible security incidents

3. All vulnerability scans will be conducted within the guidelines of the Guiding Principles set forth in the General Policy for University Information Technology Resources.

4. The IS&T Security Department will not perform Denial of Service testing in its scanning.

5. Network performance may be affected by network scanning. The IS&T Security Department will try to minimize the effect on network performance to the best of its ability.

6. The IS&T Security Department should be notified if a vulnerability scan is causing problems. See below for the points of contact.

7. The IS&T Security hot line, (216/687-5560) or the general email address (*security@csuohio.edu*), are identified as the points of contact for any questions regarding system scans.

8. Scanning will take place daily beginning at approximately 9:00 a.m. Output reporting of the scans will be produced weekly.

9. The execution, development and implementation of a fix for the vulnerabilities that are found are the responsibility of the owner of the system. If expertise to fix the problem does not reside in the department owning the systems that are identified as vulnerable, employees are encouraged to request assistance from the IS&T Security Department in the development and implementation of a remediation plan. See above for the points of contact

10. Employees are expected to cooperate fully with any Audit/Risk Assessments being conducted on systems for which they are accountable.

11. Audit/Risk Assessments will be performed on new machines before they are plugged into the CSU network.

12. Any machine found to be vulnerable, un-patched or a potential target for computer exploitation may be taken off the network until it is fixed.

Infected/Compromised Machines

1. Operating system and anti-virus updates must be automated so they require minimal input from the end user.

2. All machines that are infected with spyware must be cleansed with University approved antivirus and antispyware software.

3. All machines that are compromised must have their disks reformatted and the operating system and other programs reinstalled from scratch. When the machine is rebuilt, it must not be connected to a computer network until all software patches have been applied. This usually requires that the patches be downloaded on a separate machine, burned onto a CD and carried over to the machine being rebuilt.

   Rebuilding computers from scratch is the only way to guarantee that all hacker-written software is removed.

Security

1. Cleveland State University employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the university cannot guarantee the absolute security and privacy of data stored on university computing facilities. Users should therefore engage in safe computing practices including, but not limited to establishing appropriate access restrictions to their accounts, guarding their passwords, changing them regularly, encrypting, and backing up critical files when appropriate.

REVISION HISTORY