Cleveland State University

University Computer Hardware Policy

Desktop / Notebook / Tablet Computers

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

Every PC will run University-approved software

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

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.

Standard user accounts must not have administrative rights to university systems unless absolutely necessary and approved c / il l'is t nec

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 (& 6 8 Z L U H O H V V), 9 3 1 F R Q Q H F W H G G H Y L F H V F R P S X W H U, and any personal machines that are brought into the University and plugged intoa network port.

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

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

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

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

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

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

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.
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

- **04/07/2022**
- **05/02/2023**