COLLEGE OF ENGINEERING
CIVIL & ENVIRONMENTAL ENGINEERING
UNIVERSITY OF MICHIGAN
2350 Hayward ■ 2105 G.G. Brown ■ Ann Arbor Michigan 48109-2125
PH: 734-764-8495 ■ FAX: 734-764-4292

Standard for Computer Workstations

Standards Statement

This standard aims to establish the configuration of computer workstations operating within Civil & Environmental Engineering (CEE) so that they A) comply with university security recommendations; and B) can be sustainably supported by CEE Information Technology (IT) staff.

Who Should Read This Standard

- Faculty, staff, students, and affiliates operating a computer owned by the department.
- CEE IT support staff, who provide the IT support outlined in this standard.

Definitions

Disk encryption

Encryption is the process of encoding information to protect it. It helps to reduce the risk of unauthorized access and disclosure, as well as mitigating risks to the university and individuals in the event of loss or breach of data.

Endpoint protection software

Also known as antivirus or anti-malware, this protects computers from viruses, adware, spyware, ransomware, and other malware that might compromise accounts or lead to the loss of important data.

Hardened system

Hardening is the process of securing systems and the data stored on them against possible attack, theft, and accidental loss by following best practices and mitigating known vulnerabilities.

IT asset management software

This software supports the inventory management of IT assets, which include but are not limited to workstations, laptops, displays, accessories, and software licenses.

Vulnerability management software

This identifies software vulnerabilities, missing system patches, and improper configurations. Vulnerability scanning is limited to reviewing IT system and application configuration; it does not examine content found in emails or digital documents.

The Standard

Computers must be, at a minimum, configured with the following software configurations established by the university and CEE IT:

- Endpoint protection software
- Disk encryption
- IT asset management software
- Vulnerability management software

Departmental computers will be configured with the following standard hardened system images:

- Apple Computers: Izzy for MacOS
- Microsoft Windows Computers: CAEN Engineering Base Desktop
- Linux Computers: CAEN Linux EBD (Ubuntu or Red Hat Enterprise Linux)

To maintain high standards of security and support, departmental computers will be configured with the standard hardened system images as a default practice. However, in cases where the standard image significantly hinders the intended use or functionality for the end-user, alternative operating system deployments including the standard software packages may be granted as exceptions. Requests for such exceptions must be thoroughly justified and will require approval by the IT & Communications Committee on a case-by-case basis.

References

- SPG Policy Category: Information Technology
- SPG 601.07: Responsible Use of Information Resources
- SPG 601.27: Information Security
- DS-15: Encryption
- DS-21: Vulnerability Management
- General Information Technology Policies
- Protect Your Unit's IT
- Hardening for U-M Systems
- Encryption

Review of the Standard

The CEE IT and Communication Committee will annually review this standard and may make adjustments. CEE IT will communicate any changes to the relevant parties.

Adopted: 04/26/2024
Last reviewed: 04/26/2024