Title/Subject: **SECURE CONFIGURATIONS POLICY - WORKSTATIONS**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees □ visitors ☒ contractors

Effective Date of This Revision: January 1, 2018

Contact for More Information: Office of Information Technology

□ Board Policy ☒ Administrative Policy ☒ Procedure □ Guideline

BACKGROUND:

Central Michigan University's ("the University") workstations can contain or have access to large amounts of sensitive data regarding its students, employees, research, and other University matters. It is critical that these workstations be protected from cyber-security threats, including, but not limited to, attack, unauthorized access, misconfiguration, neglect, vulnerability exploit, and compromise. Many of the University's workstations are also required to meet regulatory compliance requirements related to cyber-security. The University needs to ensure that its workstations are configured in a manner that provides appropriate protections against these threats and is consistent with regulatory compliance requirements.

DEFINITIONS:

A. *Workstation* means any University-owned physical computer or computing device running a desktop-type operating system (e.g. MS Windows, Mac OS, Linux) used to access electronic data, including those called desktop, tower, laptop, all-in-one, and tablet-based computers.

B. *The Principle of Least Privilege* means the minimum necessary level of authority and/or access required to perform the legitimate purposes or intended functions of the applicable electronic information or system(s). This principle protects against both faults (malfunctions) and malicious behavior (misuse).

C. *Controls* are protections or safeguards implemented to protect data. Controls can be administrative, physical, and technical in nature, simple or complicated, and are often implemented in combinations or layers to protect data from simultaneous and ongoing threats.

D. *Reasonable and Appropriate Controls* means safeguards implemented to protect against reasonably anticipated threats or hazards to the security of electronic systems and information, as well as commensurate to the risk of misuse, inappropriate access, and violation of their security.

POLICY:

The Office of Information Technology (OIT) will ensure that the University's workstations are protected with a suite of best practice controls reasonable and appropriate to 1) the data on or accessed by the workstation and 2) the capabilities and purpose of the workstation itself.

In addition, the University is committed to the "Principle of Least Privilege" (see "Definitions: B" above). Standard user accounts must not have administrative rights to the workstation, and workstation administrative, super-user, and privileged-access must not be used during regular user sessions (i.e. a separate administrative account must be used for workstation administration, and administrative rights must not be granted to the user account).

Authority: George E. Ross, President
History: New Policy
Indexed as: principle of least privilege; workstations

PROCEDURE:

OIT has designed the guidance below to describe the basic safeguards that meet the requirements of this policy, as well as to indicate where additional safeguards are required. This guidance is based on the Center for Internet Security's 20 Critical Security Controls, which OIT has adopted as a standard framework of security controls.
Workstations are required to be protected with at least the following standard controls, and OIT staff have the authority to ensure these controls are in place and kept current.
Workstations used for access, processing, or storage of Restricted data (see <Data Stewardship Policy>) may require additional, specialized protection and must have those protections installed, activated, managed and kept up-to-date. Users and their IT support personnel are responsible for knowing and maintaining additional, applicable controls.
OIT recognizes that these controls may not fit the needs of all faculty and staff. In such cases, consistent with the Principle of Least Privilege and if the controls in question are not required by regulatory specification, OIT management staff can address identified needs by providing the faculty or staff member with an appropriate level of workstation access. Exceptions might include alterations to automated software updates, targeted changes to file and account access, assignment of administrative service accounts, and even, in exceptional cases, assignment of local workstation administrative accounts. Exceptions will be catalogued, regularly reviewed, modified if appropriate, and revoked if misused; they can be requested through the OIT Help Desk at 989.774.3662 or helpdesk@cmich.edu.

Standard controls include:

- **Administrative Access**
  All workstations will have OIT administrative access accounts in order for OIT to patch, update, and manage the workstations, and OIT administrative access to the workstation must not be disabled or removed until device disposal.

- **Asset Tracking**
  All workstations must be labelled and tracked via CMU property tags and network registration. Where feasible, remote-find and remote-wipe technologies should also be implemented to protect against theft or loss.

- **Configuration Management**
  All workstations must have a defined method for installing, reviewing, and managing their configurations and ensuring installed software is patched, inventoried, and up-to-date. Where feasible, configuration management methods should be automated and electronic.

- **Malware Protection**
  All workstations must run current and up-to-date anti-malware software to protect the workstation and connected devices from infection or compromise.

- **Password Protection**
  All workstations intended for exclusive use by a single user (assigned to an individual) require a strong and secret-per-user password or passcode at startup and return-from-session-timeout, to verify user authorization to use the device. Where feasible, built-in biometric capabilities (fingerprint scan, facial recognition, etc.) may be used in lieu of and/or in addition to a password.

- **Patch Management (Software Updates)**
  All workstations must use automatic or controlled patch management to stay up-to-date with at least the critical security and operational patches applicable to the workstation and its installed operating system software. All software on workstations should be patched to current release levels, and vendor-unsupported software and devices should be uninstalled or removed from use. Unpatched machines may be electronically or physically removed to quarantine (limited or no internet and network access) without prior notification. Faculty and staff with administrator-level access to their workstations should anticipate this and collaborate with OIT support staff to mitigate patch management concerns.

- **Personal Firewall**
  All workstations must have an up-to-date personal (local) firewall installed and running. It should not be disabled unless another equally-effective software or hardware device is managing or acting as the personal firewall.

- **Physical Protection**
  Users must keep all workstations and portable devices assigned to them physically protected from damage, theft, or loss at all times.

- **Proper Disposal**
  All workstations must be properly disposed of following University requirements for disposal (see Computer Disposal Policy). It must be verified that all Institutional data has been wiped or destroyed prior to final disposal.

- **Removable Media Protections**
  Users must protect all removable media containing University data from damage, theft, or loss at all times. Removable media must be disposed of properly when no longer needed or functional. Removable media from untrusted sources should not be used, and may not be used without first being scanned for malicious software. Users are responsible for ensuring that removable media containing Restricted data are encrypted and password-protected to prevent unauthorized access, loss, or theft. Faculty and staff can contact the OIT Help Desk at 989.774.3662 or helpdesk@cmich.edu for assistance with scanning or encrypting removable media.

- **Session Time-out or Screen Saver**
  All workstations intended for exclusive use by a single user must be configured to time-out and require re-authentication (login, password, biometric, or other user verification) to resume functions after idle periods of non-use. Generally, time-outs will not exceed 45 minutes but may vary depending upon risk and additional workstation protections (the more public an area, or sensitive the data and systems used, the shorter the time-out period should be). Idle session timeouts or a password-protected screen saver must be used to prevent workstation access where connected sessions to systems with Protected and Restricted data may persist.

- **User Data Backups**
  Workstations critical to departmental functions must be backed up. All workstations should be backed up to preserve user data in case of loss, storage malfunction, or damage to the device, including malicious encryption or ransomware. Backups to removable media must follow the Removable Media Protections requirement listed above. OIT will treat ransomware-encrypted workstation hard drives as failed hard drives and reload them as if new, then restore any user files from backups. If a workstation has not been backed up, all user data may be lost.

- **Whole Disk Encryption**
  Where the technologies permit, all workstations and especially portable devices should be encrypted with password-protected, whole disk encryption (also called full-disk encryption) to protect any sensitive user and Institutional data in the event or a theft or loss of the device. Encryption unlock codes or human-readable passwords may not be stored with the device. Whole disk encryption must be used on workstations where Restricted data is present.

RELATED POLICIES AND OTHER RESOURCES:

Responsible Use of Computing Policy
Data Stewardship Policy
Information Security Policy
Computer Disposal Policy
Information Security FAQ

AMENDMENTS AND ADDITIONS:

The CIO may approve exceptions to this policy. All amendments and additions to this policy will be drafted by a committee convened by the CIO and will be reviewed and approved by the Provost and the President. Changes in this policy will be appropriately publicized.

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.