Title/Subject: **SECURE SERVER CONFIGURATIONS POLICY**

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

Effective Date of This Revision: July 1, 2019

Contact for More Information: Office of Information Technology

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

BACKGROUND AND PURPOSE:

Central Michigan University's ("CMU") computing servers and systems ("servers") can contain large amounts of sensitive data regarding our students, employees, research, and other university matters. This policy has been adopted to ensure that these valuable resources are being appropriately protected from cybersecurity threats, including, but not limited to, attack, unauthorized access, data loss, misconfiguration, neglect, vulnerability exploit, and compromise.

DEFINITIONS:

CMU's Office of Information Technology utilizes the National Institute of Standards and Technology (NIST) Special Publication 800-123 to define a server: "A server is a host that provides one or more services for other hosts over a network as a primary function." For purposes of this policy, a host that does not provide services for other hosts as a primary function, but incidentally provides one or a few services for maintenance or accessibility purposes, is not considered a server. For example, a laptop that has a remote access service enabled so that IT support staff can remotely maintain it and perform troubleshooting would not be considered as a server under this policy.

POLICY:

CMU delegates the responsibility for protecting its servers to the Office of Information Technology (OIT). All University-owned servers must be protected against cybersecurity threats via implementation of a set of basic controls defined and maintained by OIT. Compensating controls for particular servers may be considered and authorized by OIT staff but will not be permitted for servers housing or processing Restricted information (see CMU's Data Stewardship Policy at https://www.cmich.edu/docs/default-source/president's-division/general-counsel/administrative-policy-docs/3/P03030.pdf for this definition). Servers without basic or compensating controls will be restricted from Internet and other forms of network access.

PROCEDURE:

OIT maintains a set of server controls and configurations that will minimally include the items below. A form for registering servers and documenting their adherence to these standards is available here: https://www.cmich.edu/docs/default-source/president%27s-division/office-of-information-technology/Secure_Server_Checklist.pdf

Ownership: All servers on the CMU network must have a clear point of contact with whom OIT can engage quickly in case of compromise or other emergency.

Authority: Robert O. Davies, President
History: New Policy
Indexed as: Secure Server Configurations

Server Inventory: The use and the classification of the data housed on each server should be documented.
Basic Controls: All servers hosting and processing institutional data are required to meet the minimum security and configuration standards for ensuring proper function and basic protection of the servers and data. These standards can be found on the checklist linked above.

Additional Controls: Servers housing Restricted data (HIPAA data, for example) require additional controls specific to restrictions, agreements, or regulations governing them.

Controls for Outdated Servers: Servers and data no longer in active use (including test and development servers and data) or unable to meet current industry practices for minimum security and configuration standards will be removed from use and properly stored or disposed of, or secured using alternative compensating controls (for instance, unplugged from the network or isolated behind a network firewall).

Plans for Monitoring Server Activity: Plans for logging server access and scanning the server for vulnerabilities should be documented.

Controls for Public-Facing Visibility: CMU IT assets are hidden from public view by default. OIT server controls will include a mechanism whereby, as an exception, the need for public visibility can be identified and managed.

ENFORCEMENT:

Each CMU department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this Policy.

The Chief Information Officer (CIO) is responsible for enforcing this policy and is authorized to set specific password creation and management standards for CMU systems and accounts.

RELATED POLICIES AND OTHER RESOURCES:

Responsible Use of Computing Policy
Data Stewardship Policy
Information Security Policy

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.