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

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

Effective Date of This Revision: July 1, 2018

Contact for More Information: Office of Information Technology

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

BACKGROUND:

CMU's networked printers can contain sensitive data regarding our students, employees, research, and other University matters, and if misconfigured and unsecured, can allow unauthorized access to CMU's computer network. It is critical that these devices be protected from cyber-security threats, including, but not limited to, attack, unauthorized access, neglect, vulnerability exploit, and compromise. This policy requires basic security controls be implemented as secure configurations on all University networked printers (wired and wireless). This policy is intended to apply to networked printers and other similar networked devices (like multi-function devices that print, scan, and copy, etc.) owned or leased by CMU, even if not specifically called "printers."

DEFINITIONS:

A. ***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.

POLICY:

All University networked printers must be secured against cyber-security threats via implementation and maintenance of a set of basic controls defined and managed by the Office of Information Technology (OIT). Controls must be commensurate to the risks and requirements of the data accessed, processed, or stored on the printer. Printers unable to meet these basic controls must be otherwise protected with compensating controls or removed from network access.

PROCEDURE:

OIT has designed the guidance below to describe the basic security controls that meet the requirements of this policy, as well as to indicate where additional security controls are required. Additional security controls (including security settings) appropriate to specific printers are detailed in the OIT Knowledge Base ("KB").

Networked Printer Basic Security Controls:

A. Remove from direct-internet access, except where intended
B. Secure from anonymous and unauthenticated access
C. Change all default, vendor-supplied passwords prior to use
D. Disable all default and non-needed services and protocols
E. Register the printers to specific, CMU-community individuals for asset tracking and support/response
F. Where feasible, configure printer setting to protect (encrypt) or completely delete stored data no longer required or no longer

---

Authority: George E. Ross, President
History: New Policy
Indexed as: network printers

being used. If printer is supported by a 3rd party or vendor, ensure stored data destruction is part of the service agreement or contract.

OIT may require more or different security controls for printers in highly controlled areas - for instance, on printers with access to or printing restricted data. These additional controls may be specified in applicable regulations or data use agreements and may include restricted physical access and continuous departmental-user oversight or supervision, and immediate removal or securing of printed materials.

RELATED POLICIES AND OTHER RESOURCES:

Responsible Use of Computing Policy
Data Stewardship Policy
Information Security 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.