

CYBERB@CIB

Title of Policy: **Responsible technology use**

Number: 3364-65-01

Issuing Officer: President

Responsible Agent: Vice President, CIO/CTO

Scope: All University of Toledo organizational units



Effective date: March 8, 2024

Original effective date:  
November 18, 2008

Keywords:

	or revision of existing policy		Reaffirmation of existing policy

**A) Policy statement**

The principles of academic freedom and freedom of expression apply to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with those principles.

Like the use of any other university -provided resource and like any other university-related activity, the use of computing resources is subject to the requirements of legal and ethical behavior within the university community. The legitimate use of a computer, computer system or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible.

Users of university computing resources shall comply with the requirements identified in this policy.

**B) Purpose**

This policy establishes requirements for the responsible use of university computing resources, identifies security enforcement and privacy measures, and potential consequences for violations.

(C) Scope

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or any device operating on a university network, or networks provided or operated by specific units of the university. Consult the operators or managers of the specific computer, computer system or network in which you are interested in for further information.

(D) Definitions

- (1) Sensitive data. Sensitive data is data with respect to which the university has an obligation to maintain confidentiality, integrity, or reliability. reli ( main)6 ((rs)2 (,)11 ( c)4 0.0 (t)

under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university.

- (3) Respect the security of sensitive data and the privacy of other users and their accounts, regardless of whether those accounts are reasonably protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
  - (a) Refrain from storing sensitive data on to portable storage devices where appropriate.
  - (b) Refrain from using elevated administrative roles to circumvent policy or university guidelines.
  - (c) Refrain from using sensitive data outside the scope of job description and duties.
  - (d) Refrain from accessing data inappropriately.
- (4) Respect the finite capacity of those computing resources and



**Approved by:**

/s/

Gregory Postel, MD  
President

**Date:** March 8, 2024

**Review/revision completed by:**

- x Vice President, CIO/CTO
- x Senior Leadership Team

**Policies superseded by this policy:**

- x Policynumber changed from 336465-05 to 336405-01 effective January 12, 2017

**Original effective date:**

November 18, 2008

**Review/revision date:**

January 12, 2017

October 26, 2020

October 11, 2023

March 8, 2024

**Next review date:**

March 8, 2027