Name of Policy: Technology incident response **Policy Number**: 3364-65-10 **Approving Officer**: President **Responsible Agent**: Vice President, CIO/CTO **Scope**: All University organizational units	THE UNIVERSITY OF TOLEDO 1872 **Effective date:** March 8, 2024 **Original effective date:** May 4, 2011

□	New policy proposal	☒	Minor/technical revision of existing policy
□	Major revision of existing policy	□	Reaffirmation of existing policy

(A) Policy statement

Technology is an integral part of how the university carries out its mission. The university must be prepared to evaluate unwanted technical events effectively and to respond appropriately when technology incidents are identified. Preparation and planning for an incident and ensuring that the right resources are available is vital to the university's ability to further prevent, detect, respond and recover from information technology incidents.

(B) Purpose

This policy defines adverse technology events and incidents and identifies their respective security response requirements.

(C) Scope

This policy applies to all university organizational units, including affiliates operating on the university technical infrastructure.

(D) Definitions

(1) Adverse event. Any observable occurrence with a negative consequence or impact to the confidentiality, integrity, or availability of a technology asset, system, or network. Examples of adverse events include system crashes, network packet floods, unauthorized use of system privileges, unexplained alteration of data, missing or unaccounted-for computing equipment, or other unexplained harmful or unwanted activity.

(2) Incident. A suspected or identified adverse event or group of adverse events, which if confirmed has or had significant potential to negatively impact the confidentiality, integrity, or availability of sensitive data or university technology assets. An incident may also be an identified violation or imminent threat of violation of a university policy. Some examples of possible information technology incidents include:

(a) Loss of confidentiality of information;

(b) Compromise of integrity of information;

(c) Loss of system availability or denial of service;

(d) Loss or theft of a technology asset;

(e) Unauthorized damage to, or destruction of, a technology asset;

(f) Unauthorized execution of, or damage to systems by, malicious code, such as viruses, trojan horses or hacking tools;

(g) Compromise of authentication data or username and password credentials;

(h) Use of university technology assets in violation of state or federal law.

(3) Incidents are categorized into two classes:

(a) Major incidents. Major technology incidents are those of significant scope or scale that affects large numbers of university technology resources and university community members, and that results in extended downtime of technology services and can cause a serious interruption to business activities and/or services.

(b) Minor incidents. Minor incidents are those incidents that do not rise to the severity or impact of a major incident, based on an impact analysis or predetermined criteria.

(c) The vice president and chief information officer/chief technology officer, in collaboration with the information technology leadership team, shall establish and revise as necessary or appropriate the university's technology incident management protocols, to be maintained within the enterprise system of record.

(4) Incident response. A structured and organized response to any information technology adverse event or incident that threatens an organization's system assets, including systems, networks and telecommunications systems.

(5) Incident response team. A group of professionals within an organization empowered to respond to identified information technology incidents.

(6) Sensitive data. Sensitive data is data for which the university has an obligation to maintain confidentiality, integrity, or availability.

(E) Policy

The university maintains an information technology incident response capability. This capability provides the ability to detect and respond to adverse events, determines if an adverse event has become an incident, determines the severity of the incident, and identifies the individuals responsible for determining how the incident is to be handled. The university's incident response capability shall include, but not limited to, the following:

a. Adverse events.

i. Incident reporting procedures. The information security office develops and maintains procedures for the reporting of adverse technology events through established channels. Absent a specific directive, adverse events may be reported through any of the incident response team organizations identified in this policy, as the situation demands. Following the initial report of an adverse event, the university organization that receives notification of a potential incident must notify the information security office of the event.

ii. Incident response procedures. The information security office must develop and maintain procedures to evaluate and determine if an adverse event has become an incident.

b. Minor incidents. All identified incidents must adhere to these general requirements:

i. Investigation. Upon discovering an incident, the information security office must make a reasonable effort to determine the scope and extent of the incident and potential threat to the security of sensitive data. In the event of an incident, the university has the authority to investigate and identify any data involved involving the relevant devices and workstations, and to the extent possible, fulfill the university's obligations to mitigate the effects of the incident. Use of the university network constitutes consent to provide access to a device in this regard, including making the equipment available to analysis and investigation by university personnel. Devices may be removed from the network to minimize further disruption.

ii. Management notification. Where applicable, documented technology incidents must be reported to appropriate management authorities within a reasonable time.

iii. Response and remediation. To the extent possible, the causes and effects of minor incidents must be identified and addressed by the appropriate IT resource.

iv. Escalation. If upon investigation a minor incident is determined to constitute a material threat to sensitive data, the incident may be escalated and handled under the major incident requirements of this policy.

c. Major incidents. In addition to the requirements of minor incidents, major incidents may comply with the following requirements:

i. Incident response team. The response to major incidents is ordinated by a flexible, situation-based, ad hoc committee, formed by the vice president and chief information officer/chief technology officer, senior leadership team, and/or functional leads as needed depending on area of incident. The university incident response team may be comprised of staff from the following university units:

a. Information technology ;
b. Privacy office;
c. Office of legal affairs;
d. Risk management and insurance;
e. Internal audit and compliance;
f. Human resources;
g. Marketing and communications;
h. University of Toledo police department;
i. Outside legal counsel upon recommendation of the university office of legal affairs and upon approval of the Ohio attorney general’s office; and
j. Outside experts;
(a) Information technology;
(b) Internal audit and compliance;

(c) Human resources;
(d) Marketing and communications;
(e) University of Toledo police department;
(f) Outside legal counsel upon recommendation of the university office of legal affairs and upon approval of the Ohio attorney general's office; and
(g) Outside experts (to the extent necessary);

ii. Response and remediation. The causes and effects of major incidents must be addressed under the direction of the incident response team assembled for the incident.

iii. Documentation. The incident response team's actions in response to an identified security incident must be documented and retained for the period proscribed by the office of legal affairs.

Approved by: /s/ Gregory C. Postel, M.D. President March 8, 2024 Date *Review/Revision Completed by:* Senior Leadership Team Vice President, CIO/CTO	**Policies Superseded by This Policy:** • *3364-65-16 Computer incident response, effective May 4, 2011* • *Policy number changed from 3364-65-16 to 3364-65-10 effective January 12, 2017* **Initial effective date:** *May 4, 2011* **Review/Revision Date:** *January 12, 2017* *October 26, 2020* *March 8, 2024* **Next review date:** *March 8, 2027*