3364-65-10 **Technology incident response 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 security 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 security 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.

(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 security 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 incidents are those incidents that pose a material threat to the security of sensitive data, based on a risk analysis or other predetermined criteria.

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

(4) Incident response. A structured and organized response to any information technology security 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 security 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 security 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:

(1) Adverse events.

(a) 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.

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

(2) Minor incidents. All identified incidents must adhere to these general requirements:

(a) Documentation. Upon being reported to the information security office, facts which constitute a minor incident must be documented within a reasonable time, and updated on a reasonable basis thereafter until closed with the determination that no material threat to sensitive data exists.

(b) 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 or alleged breach, 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.

(c) Management notification. Where applicable, documented security incidents must be reported to appropriate management authorities within a reasonable time.

~~(3)~~ (d) Response and remediation. To the extent possible, the causes and effects of minor incidents must be identified and addressed by the information security office.

~~(a)~~(e) 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.

~~(4)~~(3) Major incidents. In addition to the requirements of minor incidents, major incidents must comply with the following requirements:

(a) Incident response team. The response to major incidents is ordinated by a flexible, situation-based, ad hoc committee. The university incident response team may be comprised of staff from the following university units:

Permanent members (must be notified of any major incident regardless of the relative level of involvement with responding to a particular matter):

(i) Information security office

Under the vice president, chief information officer/chief technology officer "CIO/CTO", the information security office leads the fact gathering and technical investigation of major incidents, and

reports progress to the incident response team members and to executive leadership. The vice president, CIO/CTO serves as the senior executive interface for the technology incident response function.

(ii) Privacy office

Under internal audit and compliance, the privacy office provides coordination of major incident investigation functions across organizational lines, identifies applicable privacy concerns, monitors the progress of the investigation, and handles routine communications with regulatory bodies. This coordination is intended to enable the controlled sharing of information and the prevention of cross-purpose actions.

(iii) Office of legal affairs

The office of legal affairs serves as legal counsel to the incident response team and ensuring that the university establishes its response in a defensible manner.

(iv) Risk management

Under the office of legal affairs, the risk management administrator coordinates the relationship with the university's insurers.

(v) Ad hoc members may include any necessary resources, such as a vice president or designee with responsibility for a university organizational unit, or authorized third parties, including:

(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);

(b) 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.

(c) 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.

Effective: 12/14/2020

CERTIFIED ELECTRONICALLY

Certification

12/02/2020

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364
Prior Effective Dates:	04/01/2018