3364-65-02 Information security and technology administrative safeguards policy.

(A) Policy statement

The university of Toledo places the utmost importance on the privacy rights of its students, patients, faculty, staff, and community members and takes the security of information very seriously. To protect the confidentiality, integrity, and availability of stakeholder information, the university has implemented a framework for an effective and efficient information security program, and supports the framework through a comprehensive body of technology policies and procedures that serve to:

(1) Promote the public trust;

(2) Ensure continuity of university services;

(3) Recognize and mitigate risks and threats to the institution and its stakeholders;

(4) Comply with legal and contractual requirements;

(5) Protect sensitive information and technology assets from loss of confidentiality, integrity, and availability.

(B) Purpose

The university of Toledo information security program is designed to identify and mitigate threats to information security and privacy. This policy and its supporting policies and procedures provide a foundation for the program. The requirements described in this policy and its subordinate policies and procedures are intended to ensure that due diligence is exercised in the protection of information, systems and services, and that the university's information security program meets certain requirements enforced by law. This policy describes fundamental practices of information security that must be applied by university organizations under the guidance of the university's information security office to ensure that protective measures are implemented and maintained.

(C) Scope

The scope of this information technology policy applies to all university operating units, and includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.

(D) Definitions

(1) Access control list. A list of entities and their authorized access rights to an information resource.

(2) Authentication. The process or action of proving the identity of an entity (such as a person, computer, system or process) based on one or more factors.

(3) Authorization. A grant to a requesting entity (computer, system, person or process) for access to a protected system and its resources.

(4) Availability. The assurance that information and services are delivered when needed.

(5) Biometrics. Biological characteristics such as fingerprint, face or retinal blood vessel patterns used by authentication devices to allow an individual access to information, services or other resources.

(6) Cardholder data. Cardholder data "CHD" means the subset of sensitive data comprised of the university's identifiable payment card information (e.g., credit cards, debit cards, and stored value cards related information).

(7) Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information.

(8) Custodian. Custodians are the named individuals or job titles responsible for making access control decisions.

(9) Data. Electronically coded representation of quantities, objects and actions. The word, “data,” is often used interchangeably with the word, “information,” in common usage and in this policy.

(10) Device. As used in this policy, “Device” shall retain its meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(11) Digital certificate. An electronic document used for security purposes to authenticate the sender or recipient of information, or to authenticate the contents of the information itself.

(12) Electronic protected health information. Electronic protected health information “ePHI” means protected health information accessed, stored, processed, transmitted, or received in electronic format. Protected health information “PHI” means the subset of sensitive data comprised of the university’s patient data and other identifiable health information, for which the university is obligated to maintain confidentiality, integrity, and availability under the Health Insurance Portability and Accountability Act of 1996 and subsequent laws and regulations.

(13) The Family Educational Rights and Privacy Act of 1974 “FERPA,” as amended is a federal law that protects the privacy of education records of all students enrolled in schools beyond the high school level. Schools are required to maintain that privacy, primarily by restricting release of records and the access provided to those records. Any educational institution that receives funds under any program administered by the U.S. Secretary of Education is bound by FERPA requirements. Institutions that fail to comply with FERPA may have funds administered by the Secretary of Education withheld. The U.S. Department of Education maintains a website with information about FERPA.

(14) Firewall. Either software or a combination of hardware and software that implements network security policy with respect to communication between two or more networks or network segments.

(15) Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act.

(16) Information technology asset. Information technology assets "IT assets" shall retain their meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management Policy).

(17) Least-privilege. A model for assigning privileges in a system with the objective that only those privileges necessary to perform a required function are assigned, and ensure that other privileges are not assigned and cannot be improperly accessed.

(18) Malicious software. Malicious software "malware" is a collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, ransomware, trojan horses and worms.

(19) Multi-factor authentication. Authentication of an entity based on two or more distinct elements.

(20) Payment card industry data security standards. Payment card industry data security standards "PCI-DSS" means the body of legal and contractual requirements placed on the university relating to the security and privacy of cardholder data.

(21) Personally identifiable information. Personally identifiable information "PII" refers to information that may be used, on its own or in combination with other information, to uniquely identify a natural person, regardless of any obligation (or lack thereof) for the university to maintain confidentiality, integrity, or availability.

(22) Risk assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization.

(23) Risk management. A discipline concerned with the planning, implementing and monitoring of processes for the identification, measurement, control and minimization of security risks to information systems at a level commensurate with the value of the assets to be protected.

(24) Security token. A portable, physical device that enables pre-approved access to data or systems. An example is a security-enabled key fob.

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

(26) Technology asset. Technology assets shall retain their meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(27) Threat. An event, whether artificial or natural, with the potential to cause harm to a technology asset.

(28) Two-factor authentication. Authentication of an entity based on two distinct elements.

(29) Users. Employees, students, contractors, temporary personnel and other affiliates of the university who administer or use privately-owned (if authorized) or university-owned computer and telecommunication systems on behalf of the university.

(30) Vetting process. A verification process used to validate the identity and trustworthiness of a person who is seeking access to computer systems and networks.

(31) Workstation. As used in this policy, "workstation" shall retain its meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(E) Policy

Under the direction of the information security officer, the university will establish and maintain an information security program to carry out the security and privacy objectives of the institution. University organizations must exercise due diligence to ensure that technology assets that conduct or support the university's mission are reasonably secure, and that the information contained within those assets is protected from unauthorized disclosure, modification or destruction, whether accidental or intentional.

(1) Program administration. The university has established an administrative structure to support the information security program.

(a) Organizational structure.

(i) Executive sponsorship. The vice president, chief information officer/chief technology officer "CIO/CTO" serves as the chief executive for university technology and is the principal sponsor of the information security program.

(ii) Information security office. Reporting to the vice president, CIO/CTO, the information security officer "ISO" serves as the university's lead cybersecurity official, directs the functions of the university's information security office, and coordinates information security activities across university organizational lines. For purposes of the Health Insurance Portability and Accountability Act and related law and regulation (collectively, "HIPAA"), and the Family Educational Rights and Privacy Act (collectively, "FERPA"), the ISO is also designated as the security official for the university's covered entity components.

(iii) Assurance. The senior director, internal audit and chief compliance officer serves as the principal examiner of the security program to assure that it is in alignment with the university's requirements.

(b) Management process. The ISO is responsible for developing, implementing, managing, and maintaining an information security framework, based on industry best practices, legal, and contractual requirements. The information security framework is intended to identify, prevent and protect against, detect and contain, respond and recover from security threats, risks, and incidents. Elements of the framework include:

(i) Risk analysis. The ISO will establish procedures to conduct assessments of risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive data.

(ii) Risk management. In partnership with the university's risk management function, the ISO will implement an adequate security program to manage risks and vulnerabilities identified through risk analysis to sensitive data. These risk management measures may include risk avoidance, risk mitigation, risk transfer, and acceptance of risk.

(iii) Continuous improvement. The ISO improves the security program based on outcomes from incidents and investigations, and internal and external assessments.

(2) Program Principles. The following general principles provide the foundation for university security policy development:

(a) Accountability. While the ISO guides the overall direction of the information security program, technology asset owners within university organizational units retain ultimate responsibility for the confidentiality, integrity, and availability of data.

(b) Risk orientation. The vice president, CIO/CTO ensures that the information security program aligns with the university's strategic objectives and to the university mission. To achieve this alignment, the ISO coordinates with university organizational units to apply risk management techniques in order to balance the need for security measures against these strategic objectives in proportion to the risk presented.

(c) Least privilege to sensitive data. Security measures provide an adequate level of access to sensitive data necessary to accomplish the legitimate purposes of the organization, but no more access than is necessary. University organizations must provide sensitive data only

to those that are authorized and have a valid institutional need for the information.

(d) Confidentiality, integrity and availability. University organizations shall ensure that their security practices address the basic security elements of confidentiality, integrity and availability to an appropriate degree, as determined by risk analysis. To this end, university organizations must:

(i) Ensure the confidentiality of information to a reasonable degree, such that it is not accessible beyond legally permissible or university accepted limits.

(ii) Ensure the integrity of information and services to a reasonable degree, so that it is not altered beyond legally permissible or university accepted limits.

(iii) Ensure that information and services are available to a reasonable degree, and within the parameters prescribed by legally permissible or university accepted limits described in applicable rule 3364-65-09 of Administrative Code (technology backup, disaster readiness and recovery).

(3) Program activities. The information security office carries out the following activities:

(a) Identify risks, threats, and vulnerabilities. The information security officer directs program activities related to identification and assessment of security risks, threats, and vulnerabilities.

(i) Discovery and identification. The security program relies on technical and non-technical means to discover, identify, and classify technology assets and security risks, threats, and vulnerabilities to technology assets.

(ii) Assessment and evaluation. The security program relies on quantitative and qualitative assessment and evaluation techniques to gauge the relative harm presented by an identified risk, threat, or vulnerability, and recommends measures to manage the risk, threat, or vulnerability.

(iii) Policy and procedure reviews. The security program reviews the body of security-related university of Toledo IT policies and procedures, and implements updated provisions as required.

(b) Prevent and protect the university from identified threats and risks.

(i) Preventative controls.

The security program implements and maintains controls intended to prevent the exploitation of vulnerabilities and the realization of security risks.

(ii) Protective controls.

The security program implements and maintains controls intended to protect against threats, natural and artificial.

(c) Detect security incidents.

Detective controls. The information security program implements and maintains controls to detect when system assets are safe and when they are threatened. These controls include activity monitoring and auditing of technology assets at appropriate intervals.

(d) Respond to security incidents.

Incident readiness and response. The information security program implements and maintains safeguards intended to prepare for and identify, classify, and respond to

technology incidents.

(e) Recover from security incidents.

Incident recovery. The information security program implements and maintains protocols/procedures designed to ease the recovery from a technology incident and to incorporate new lessons learned into future incident response procedures.

(4) Administrative safeguards. To carry out the information security program, these administrative safeguards are required to ensure that human and process controls exist to protect sensitive data.

(a) Risk management. Under the direction of the ISO, the university conducts security risk management activities to permit informed decision-making with respect to its ongoing technology activities and to limit overall risk to acceptable levels.

(i) Risk analysis. The ISO is responsible for performing a periodic risk assessment to gauge the overall security posture of the institution. The ISO provides the findings of the risk analysis to the university's privacy and security committee not less than annually.

(ii) Risk assessment. Upon discovery of an adverse event that could constitute the material breach of Sensitive Information, an incident response team is formed as described in rule 3364-65-10 of the Administrative Code (technology incident response). Guided by the ISO's findings, the incident response team performs an analysis of the risk of loss of confidentiality, integrity, or availability.

(iii) Security evaluations. Under the direction of the ISO, the university performs technical and non-technical evaluations of the security program and of the university's operating environment. These

evaluations may include invasive physical and logical testing of the university's technology assets.

(iv) Risk management. Based on the findings of the university's various security risk assessment and evaluation activities, the ISO will coordinate an appropriate strategy to manage the risk, such as risk avoidance, risk transfer, risk mitigation, or risk acceptance.

(b) Identity and access management. The university relies on an identity and access management system based on unique user account identification to assign technology resources to the appropriate entity.

(i) Unique identification. User accounts must be unique and identifiable to an individual person or entity. Except as otherwise excepted, the university of Toledo active directory "UTAD" account name will serve as the unique identifier for access to technology resources.

(ii) Identity verification. User identities must be validated before issuing user IDs and other credentials. Validation procedures are established for maintaining and managing system user IDs, including procedures for establishing new user accounts, validating existing user accounts, and terminating former user accounts.

(iii) Account integrity. Except as required by law or regulation, the university does not guarantee the integrity of accounts or account credentials. Reasonable measures to protect sensitive data from unauthorized access and alteration are implemented to the necessary degree identified through risk analysis.

(iv) Role based access controls. Where appropriate or otherwise required by law or regulation, the identity and access management system provides identity

information sufficient to restrict access to sensitive data based on the functional role of the user.

(c) Authentication. The university has established authentication requirements for technology assets, which prompt the user to present one or more credentials before granting access to sensitive data.

(i) Authentication factors. Except as directed by the Vice President, CIO/CTO or the ISO, at least one authentication factor must be provided to access a technology asset. The UTAD account password serves as the default authentication factor for access to technology assets except as otherwise accepted based on a risk analysis.

(ii) Multi-factor authentication. Based on risk analysis activities, the university may require two or more authentication factors before user being granted access to a system or service that processes, transmits, or receives sensitive data. These factors may include:

(a) Passwords, passphrases, PINs, secret codes ("something you know")

(b) Tokens, smart cards, digital certificates ("something you have")

(c) Biometric factors ("something you are")

(iii) Integrity of authentication credentials. The information security office oversees the development and maintenance of procedures to manage the integrity of security credentials, such as authentication tokens and passwords. It is a violation of rule 3364-65-01 of the Administrative Code (technology responsible use), to disclose authentication factors (such as passwords), without authorization.

(iv) Passwords. The ISO establishes and maintains procedures and standards for password strength, based on a risk analysis. Except as otherwise directed by the vice president, CIO/CTO, ISO, or delegate, technology assets that create, store, process, transmit, receive, or destroy sensitive data and rely solely on the use of password authentication.

(v) Recovery of authentication credentials. The ISO establishes and maintains procedures and standards for recovery of authentication credentials, based on a risk analysis. Except as otherwise directed by the by the vice president, CIO/CTO, ISO, or delegate, a user may be required to re-validate their identity before being allowed to recover authentication credentials.

(vi) Digital signatures. Digital signatures may be used for identification and authentication pursuant to university policy and rule 123:3-1-01 of the Administrative Code.

(d) Authorization and supervision. Not all entities will have access to all university data. The university has established authorization requirements for technology assets, which implement logical and physical authorization policies and procedures to protect sensitive data and to address the management of permissions to access the various system components.

(i) Authorization. Users must be authorized to access sensitive data before being granted any access to the data. This authorization may be granted or revoked by either a manual or automatic process, and may extend to either an individual or a particular class of users (e.g., based on job role). Authorization records may be maintained by manual or automated processes.

(ii) Supervision. Ongoing authorization for user access to sensitive data may be required. Some technology assets may require ongoing authorization certifications or approvals by the university entity responsible for the data.

(iii) Role-based access. Where appropriate as determined by a risk analysis, or otherwise required by law or regulation, access to sensitive data may be strictly limited to users based on their individual user role, in accordance with the least-privilege principle.

(iv) Technology assets which access, create, process, transmit, receive, or destroy sensitive data must be configured to deny unauthorized transactions by any user. Unauthorized attempts to access sensitive data are logged and may be escalated for further investigation.

(e) Accounting and security audit logging controls. To maintain a consistent and reliable record of system activity, security audit logging capabilities on technology assets that access, create, process, transmit, receive, or destroy sensitive data are required.

(i) Audit records. The ISO establishes and maintains security audit features for technology assets and configures the audit features to sufficiently identify the user accessing the asset, the time and location of the access, attempts and failures to access the asset, and identify violations of university policy.

(ii) Review of audit records. The ISO establishes and maintains appropriate processes to review and analyze activity logs commensurate with the risk associated with the source system.

(iii) Security of audit records. Audit logs shall be protected from tampering and available for review. The ISO must ensure the confidentiality, integrity,

and availability of audit information commensurate with the risk associated with the source system.

(iv) Separation of duties. Where possible, the ISO enforces a separation of duties between personnel administering and authorizing access controls functions and those administering security audit logging functions. If these functions cannot be separated, where necessary university organizations must document the reasons and develop a process to address conflict of interest concerns.

(v) Retention of audit logs. The ISO determines an appropriate data collection scheme and retention schedule for audit logs sufficient to associate specific users with logged events, based upon a deliberate assessment of the legal and organizational requirements, asset capabilities, administrative burden, and overall risk. Logs subject to an investigation must be preserved as long as needed.

(f) Human resources. The university will establish and maintain appropriate security measures to manage security risks sourced from internal actors:

(i) Clearance procedures. Before being granted access to sensitive data, the requesting user must be cleared by the university officer responsible for the data being requested. Where clear documentation of clearance requirements exist and has been established by the custodian in advance, this clearance procedure may be delegated, as appropriate, to a university staff member responsible for provisioning user access to the data.

Where required by law or regulation, individuals with access to sensitive data may be subjected to a vetting process that is commensurate with the type of data.

(ii) Termination procedures. The university user accounts with access to sensitive data are subject to procedures which result in termination of such access after the user is no longer affiliated with the university or when the user's affiliation with the university changes.

(iii) Awareness and training. The ISO oversees the creation of security awareness and training materials. These materials include basic security topics, such as:

(a) General notices and reminders. Upon the discovery of significant new security threats, the ISO may send appropriate communications to the university community. To maintain a high degree of security awareness, the ISO also initiates periodic communications concerning common security topics and general computing tips and best practices.

(b) Malicious software. Security awareness and training materials include information related to malicious software, and the appropriate user response to a suspected malware infection.

(c) Login monitoring. Security awareness and training materials include information related to ongoing user account and login monitoring.

(d) Password management. Security awareness and training materials include information about proper password management techniques.

(e) Phishing and Fraud. Security awareness and training materials include information about

e-mail phishing and fraud techniques.

(iv) Sanctions. Violations of university policy reported to the university information security office are referred to the appropriate university disciplinary authority.

(g) Incident policies and procedures. In anticipation of technology incidents, the university maintains rule 3364-65-09 of the Administrative Code (technology backup and disaster readiness and recovery policy). In the event that a technology incident is detected, the university maintains an information technology security incident response capability, described in rule 3364-65-10 of the Administrative Code (technology incident response policy). Policies and procedures subordinate to these must include the following requirements, as appropriate.

(i) Response and reporting. The response to incidents and the reporting of incidents are conducted as described in the technology incident response policy.

(ii) Contingency plans. The university maintains adequate contingency plans to deal with adverse technology events reasonably expected in the course of the university's activities.

(a) Backup plans. Technology contingency plans include the provisions for backup of the university's sensitive data in some circumstances. Backup of sensitive data is conducted as described in the university's technology backup and disaster readiness and recovery policy.

(b) Disaster readiness and recovery plans. Technology contingency plans include the preparation for certain types of disasters reasonably foreseen by the university. The creation and maintenance of disaster

readiness plans is conducted as described in the university's technology backup and disaster readiness and recovery policy.

(c) Emergency mode operations plan. University business units which access, store, transmit, or receive PHI must establish and maintain procedures to ensure continuity of critical functions while operating in an emergency mode. While operating in emergency mode, university units must continue to protect the security of electronic health information.

(d) Testing and revision procedures. The contingency plans include testing and revision procedures for certain types of incidents reasonably foreseen by the university. These plans may include periodic or ad-hoc backup tests and disaster readiness tests, the results of which are used to incrementally improve existing procedures.

(e) Application and criticality analysis. The contingency plans for applications which access, process, transmit, or receive PHI include a reasonably accurate analysis of the criticality of the application.

(h) Legal and compliance. The information security program attempts to comply with all applicable laws, regulations, contractual requirements, and best practices, including:

(i) Federal law and regulation.

(a) The Family Education Rights and Privacy Act of 1974, ("FERPA"); (20 U.S.C. § 1232g; 34 CFR Part 99).

(b) FISMA. Federal Information Security Management Act of 2002 (Public Law 107-347, Dec. 17, 2002, 116 Stat. 2946)

(c) The Health Insurance Portability and Accountability Act of 1996, ("HIPAA"); Pub.L. 104–191, 110 Stat. 1936.

(d) National Institute of Standards and Technology Special Publication 800-30, "Risk management guide for information technology systems."

(ii) State Law

(a) Chapter 1306 of the Revised Code and Rule 123:3-1-01 of the Administrative Code specifically govern the use of legally binding records and signatures in electronic formats and include companion security requirements to this policy.

(b) Chapter 1347 of the Revised Code includes security provisions that require state agencies to, among other things, "take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use, or disclosure."

(c) Security records. Chapter 149 of the Revised Code includes provisions with regard to records management requirements and public records requirements. Section 149.433 of the Revised Code specifically addresses IT security records.

(d) Electronic signatures. Chapter 1306 of the Revised Code and Rule 123:3-1-01 of the Administrative Code specifically govern the use of legally binding records and signatures

in electronic formats and include companion security requirements to this policy.

(iii) Contracts.

(a) Procurement agreements. The university maintains its security requirements through written agreements with its vendors and technology providers

(b) Other contracts and agreements. The university requires agreements to which it is a party to contain adequate measures to protect the confidentiality, integrity, and availability of sensitive data.

(i) Physical controls. In addition to the administrative requirements described in this policy, technology assets must meet the physical security requirements described in rule 3364-65-03 of the Administrative Code (technology physical safeguards), where applicable.

(j) Logical controls. In addition to the administrative requirements of this policy, technology assets must meet the technical security requirements described in rule 3364-65-04 of the Administrative Code (security access safeguards), where applicable.

Effective: 3/11/2019

CERTIFIED ELECTRONICALLY

Certification

03/01/2019

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364