


| | | | |
|---|-----------------------------------|---|---|
| Name of Policy: <u>Information security framework.</u> Policy Number: 3364-65-13 Approving Officer: President Responsible Agent: Vice President of Information Technology Scope: all University campuses | |  Review date: December 10, 2012 Original effective date: May 28, 2009 | |
| <input type="checkbox"/> | New policy proposal | <input type="checkbox"/> | Minor/technical revision of existing policy |
| <input type="checkbox"/> | Major revision of existing policy | X | Reaffirmation of existing policy |

(A) Policy statement

The University of Toledo will support a comprehensive body of effective and efficient information technology security policies and procedures that serve to:

- (1) Promote public trust
- (2) Ensure continuity of university services
- (3) Comply with legal requirements
- (4) Recognize risks and threats
- (5) Protect system assets

(B) Purpose

The University of Toledo, "Information Security Framework," is intended as a tool to mitigate increased risks.

This policy and its supporting policies provide a foundation for the security of university information technology systems. The requirements put forth in this policy and its supporting policies are designed to ensure that due diligence is exercised in the protection of information, systems and services. This policy describes fundamental practices of information security that are to be applied by university organizations to ensure that protective measures are implemented and maintained.

(C) Scope

The scope of this information technology policy 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) Requirements

University organizations shall exercise due diligence to ensure that computer and telecommunications systems and services that conduct or support university functions are secure, and that the information contained within those systems and services is protected from unauthorized disclosure, modification or destruction, whether accidental or intentional.

- (1) The following minimum security requirements provide the foundation for university security policy development and are described in more detail in this policy.
 - (a) Risk management: Organizations shall apply risk management techniques to balance the need for security measures (paragraph D (2)(a)).
 - (b) Confidentiality, integrity and availability: Organizations shall ensure that their security policies, plans and procedures address the basic security elements of confidentiality, integrity and availability (paragraph D (2)(b)).
 - (c) Protect, detect and respond: Security plans and policies shall include methods to protect against, detect, and respond to threats and vulnerabilities to university information and systems (paragraph D (2)(c)).
 - (d) Identification and authentication: University information technology systems shall implement an identification and authentication process for information systems and services (paragraph D (2)(d)).
 - (e) Access control and authorization: Access control and authorization policies, plans and procedures are required to protect system assets and other information resources maintained by the university (paragraph D (2)(e)).
 - (f) Security audit logging: Security audit logging capabilities on information systems, including computers and network devices, shall be implemented and utilized in accordance with the risk assessment (paragraph D (2)(f)).
- (2) Minimum security requirements:
 - (a) Risk management. Organizations shall adopt a risk management methodology that incorporates the following risk management processes:
 - Risk assessment positions organizations to determine effectively the extent of potential threats and the associated risk. The goal of conducting a risk assessment is to identify organization-specific controls that are appropriate for reducing or eliminating risk;
 - Risk mitigation addresses the prioritization, evaluation and implementation of strategically selected controls. The goal of risk mitigation is to select and implement controls that reduce risk to an acceptable level; and

- Evaluation and assessment is a process comprised of activities that recognize and respond to new and changing risks, measure the effectiveness of implemented controls, and modify controls to reflect changes in the three aspects of risk management: operational, technical and managerial. The goal of evaluation and assessment is to maintain a successful and effective risk management program that continuously evolves and responds to changing threats and opportunities.

Risk management offers a practical approach to balancing security with operational requirements and cost. The definition of acceptable risk and the approach to managing risk can vary for each organization. Risk management is a trade-off in which a certain amount of residual risk is accepted as a balance to the costs of incremental countermeasures.

The likelihood that adverse events will occur is determined by analyzing possible threats in conjunction with vulnerabilities and potential business impact. The formula that follows is commonly applied by the information security community to define and measure such risks as a part of risk management. The formula further expresses the relationship of risk exposure factors to counterbalancing security strategies in defining the level of risk:

$$\text{Risk} = \frac{\text{Impact x Threats}}{\text{Countermeasures}}$$

Risk factors are defined for each system being measured and receive relative ratings of high (H), medium (M), or low (L).

As an example, risk factor ratings for a hypothetical web server that is linked to patient records might be as follows:

- Impact – The impact of a successful attack to obtain or change records might be rated as “high.”
- Threat – The likelihood of an attack might be rated as “medium.”
- Countermeasures – Alternative measures are robust and therefore would be rated as “high.”

In this hypothetical example, the robustness of the countermeasures may reduce or mitigate the overall risk, resulting in an acceptable level of risk.

- (i) Organization risk management practices shall include the elements described below.
 - (a) Risk assessment.

All university organizations shall periodically conduct a risk assessment of system assets that they maintain to address changing threats and organizational priorities. Risk assessments shall:

- Identify IT systems, resources and information that constitute each system and prioritize the relative importance of the system assets;
- Identify and document potential threat-sources;
- Identify and document system vulnerabilities that could be exploited;
- Analyze security controls that have been implemented or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring;
- Determine the likelihood of potential vulnerabilities being exercised by a threat-source;
- Determine the impact associated with the compromise of system assets;
- Determine the level of risk using a rating methodology such as high–medium–low;
- Identify technical, operational and management controls that can mitigate or eliminate the identified risks; and
- Document risk assessment results and control recommendations.

(b) Risk mitigation

University organizations shall prioritize the implementation of mitigation actions based on the results of the risk assessment. Risks may be eliminated, mitigated, shared with one or more third parties, or accepted. If certain risks are to be eliminated or mitigated the organization shall:

- Evaluate and compare the security countermeasures available, and the resources required to implement them, with the resources required to replace the system assets.
- Determine which countermeasures are reasonable to employ.
- Establish guidelines for implementing management, operational and technical security controls commensurate with the established risk to system assets.

(c) Evaluation and assessment

University organizations shall periodically evaluate security controls to determine their ongoing appropriateness and effectiveness for current and anticipated risks and update controls based upon the findings.

(b) Confidentiality, integrity and availability.

University organizations shall ensure that internal security policies, plans and procedures address the fundamental security elements of confidentiality, integrity and availability. Students, patients, and employees expect that sensitive information about them will be shared only with those who need access, that the information will not be altered either by accident or malicious intent, and that it will be available when needed. To this end, university organizations shall:

- (i) Provide information and services only to those that are authorized and have a valid business need.
- (ii) Protect information so that it is not altered maliciously or accidentally.
- (iii) Ensure that information and services are provided in conjunction and accordance with business continuity plan.

(c) Protect, detect and respond.

IT security plans and policies shall include methods to protect against, detect and respond to threats and vulnerabilities. At a minimum, organizations shall:

- (i) Determine how much protection is needed and for how long, per the results of the risk assessment and then develop policies and procedures accordingly.
- (ii) Review the body of security-related University of Toledo IT policy and implement its provisions as required.
- (iii) Develop a methodology to detect when system assets are safe and when they are threatened. The methodology needs to include auditing and recording the status of all protected system assets at intervals appropriate to the risk as defined in the assessment.
- (iv) Develop a security incident reporting procedure describing how to respond to security incidents that addresses “who,” “what,” “when,” “where” and “how,” in accordance with university policy on “Security Incident Response.”
- (v) Identify the types of services and protocols permitted by the network systems, both within the network and crossing the network boundary. The fundamental policy strategy for services and protocols external to the

network must be to “deny everything” and allow only specific services and protocols on a case-by-case basis. University organizations shall employ security precautions for the management of such services pursuant to university policy on “Boundary Protection.”

(d) Identification and authentication.

Based upon the risk assessment, university organizations shall implement an Identification and authentication (I&A) process for information systems and services that require controlled access. The identification process shall require the user to present a valid identity using a recognizable method. The most common form of identification is a user ID. The authentication process shall require the user to present verification of identity in a recognizable format. The most common form of authentication is a password. For I&A, university organizations shall meet the requirements listed below.

- (i) System users shall have unique and individual user IDs.
- (ii) User identities shall be validated before issuing user IDs and other credentials. Procedures shall be 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) All user credentials shall be protected from unauthorized access and alteration.
- (iv) A security credentials management process shall be developed that ensures the confidentiality, integrity and availability of security credentials such as passwords, PINs, biometrics, tokens and certificates. Password processes shall fulfill the requirements of university policy on “Password Security.”
- (v) If a user is locked out of a system due to a forgotten password, data entry mistake while entering a password, or any other legitimate error, organization procedures shall verify valid identification and authentication before permitting access.
- (vi) If a university organization is using, sending or receiving legally binding electronic records or signatures, the I&A process shall comply with rule 123:3-1-01 of the Ohio Administrative Code.
- (vii) An authentication process commensurate with the risk assessment of the system assets shall be established. Robust methods of authentication, such as two-factor authentication or digital certificates, should be considered to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm.

(e) Access control and authorization.

University organizations shall implement access control and authorization policies, procedures and plans to protect university information resources. Access control addresses the securing of systems, both the hardware components and the software components. Authorization addresses the management of permissions to access the various system components, including processes for approving access and restricting access. Restricting access can apply to both invalid users and valid users with limited privileges. To this end, university organizations shall:

- (i) Secure system assets from physical access by unauthorized persons at all times. At a minimum, system assets shall be in the control of authorized personnel or protected by a locking mechanism.
 - (ii) Manage systems with appropriate access control processes and well-formulated access control lists.
 - (iii) Use the least-privilege method for granting access to system assets.
 - (iv) Subject all personnel with access to system assets to a vetting process that is commensurate with the system assets risk assessment.
 - (v) Ensure that systems can detect and deny unauthorized transaction attempts by any user. Unauthorized attempts shall be logged in accordance with the security audit logging requirements defined in paragraph (f) below.
 - (vi) Implement any restrictions to accessing systems outside of normal working hours.
 - (vii) Ensure that the access control methodology can disable user privileges to those who no longer require access.
- (f) Security audit logging.

University organizations shall implement security audit logging on information systems such as computers, network devices, routers, firewalls, and applications. Audit logging shall be commensurate with the organization's risk assessment findings.

The purpose of audit logging is to maintain a consistent and reliable record of system activity. When properly implemented, audit logging can serve as a preventive measure as well as a forensic aid. A comprehensive record of "who-did-what-when" can discourage asset abuse or be a vital form of evidence to prove culpability or prosecute a perpetrator. University organizations shall:

- (i) Enable security audit features for system assets and configure them to be sufficient to track attempted security breaches. Organizations shall ensure that their audit strategy captures the information necessary to identify who is accessing university system assets,

access attempts and failures, and violations of security policy. Appropriate processes shall be put in place to review and analyze the logs commensurate with the organization's risk assessment. Audit logs shall be protected from tampering and available for review.

- (ii) Ensure the confidentiality and security of audit information.
- (iii) Ensure a separation of duties, where possible, between personnel administering access control functions and those administering security audit logging functions. If these functions cannot be separated, organizations shall document the reasons and develop a process to address conflict of interest concerns.
- (iv) Ensure that audit logs capture information sufficient to satisfy an inquiry to determine timing, events, impact and ownership of both normal system activity and violations of policy, whether security-related or business-related. Based upon a deliberate assessment of the organization, application, information and risk, determine an appropriate data collection scheme and retention schedule for audit logs sufficient to associate specific users with events that breach protocol. If logs are subject to an investigation, they shall be preserved as long as needed.

(E) Definitions

- (1) Access control list. A list of entities and their authorized access rights to a resource.
- (2) Authorization. A grant to a requesting entity (computer, system, person or process) for access to a protected system and its resources. Not all entities will have access to all university information. Authorization requirements can be implemented using techniques such as access control lists, file and resource permissions, and digital certificates.
- (3) Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.
- (4) 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.
- (5) Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure

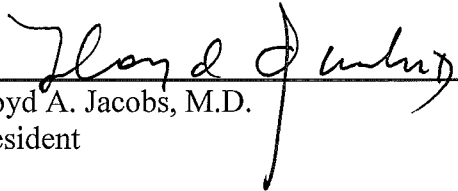
specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

- (6) Data. 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.
- (7) Digital certificate. An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.
- (8) Firewall. Either software or a combination of hardware and software that implements security policy governing traffic between two or more networks or network segments. Firewalls are used to protect internal networks, servers and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a notebook computer, and must be configured properly to enable protection.
- (9) Identification and authentication. The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques, such as user ID, password, personal identification number, digital certificates, security tokens or biometrics, to enforce I&A, depending upon the level of access control required to protect a particular system.
- (10) Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because students, patients, and employees depend upon the accuracy of data in university databases, organizations must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.
- (11) Least-Privilege. A method for assigning privileges in a system. The objective is to assign only those privileges that are necessary to perform the required functions, and ensure that other privileges are not assigned and cannot be improperly accessed. For example, a typical system user should not be assigned rights to read, write and execute all of a department’s files when the user only requires the ability to read a subset of these files to do an assigned job.
- (12) Malicious code. 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, Trojan horses and worms.

- (13) 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. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security.
- (14) 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. Risk management attempts to maximize the results of positive events and minimize the results of adverse events.
- (15) Risk mitigation. A systematic methodology used to reduce risk by employing one of the following risk options: risk assumption, risk avoidance, risk limitation, risk planning, risk transference.
- (16) Security controls. Management, operational and technical policies, procedures and tools required to achieve and maintain the necessary level of assurance of confidentiality, integrity and availability.
- (17) Security token. A portable, physical device that enables pre-approved access to data or systems. An example is a security-enabled key fob.
- (18) System assets. Information, hardware, software and services required to support the business of the university, and identified during the risk assessment process as assets that need to be protected.
- (19) Threat. An event with the potential to cause harm to an information technology process or service. A threat can be natural, human or environmental.
- (20) Two-factor authentication. Authentication that incorporates two elements. There are three elements of authentication: “what you know” (for example, a password or PIN), “what you have” (for example, a digital certificate or a smart card), and “what you are” (for example, a biometric). Two-factor authentication is commonly used for access to systems that contain data requiring secure access or information when disclosure would cause serious disruption or harm. It is also known as strong authentication, although strong authentication can have more than two elements.
- (21) Users. For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the university who administer or use privately-owned (if authorized) or university-owned computer and telecommunication systems on behalf of the university.
- (22) Vetting process. A verification process used to validate the identity and trustworthiness of a person who is seeking access to computer systems and networks.

(F) Related resources and references

- (1) Federal Information Security Management Act of 2002 (Public Law 107-347, Dec. 17, 2002, 116 STAT. 2946)
- (2) National Institute of Standards and Technology Special Publication 800-30, "Risk Management Guide for Information Technology Systems."
- (3) Chapter 1306 of the Ohio Revised Code and Rule 123:3-1-01 of the Ohio Administrative Code specifically govern the use of legally binding records and signatures in electronic formats and include companion security requirements to this policy.
- (4) Chapter 1347 of the Ohio 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."
- (5) Chapter 149 of the Ohio Revised Code includes provisions with regard to records management requirements and public records requirements. Section 149.433 of the Ohio Revised Code specifically addresses IT security records.

| | |
|---|--|
| <p>Approved by:</p>  <p>Lloyd A. Jacobs, M.D. President</p> <p><u>December 10, 2012</u> Date</p> <p>Review/Revision Completed by: Vice President of Information Technology</p> | <p>Policies Superseded by This Policy:</p> <p>Previous 3364-65-13, effective date May 28, 2009</p> <p>Initial effective date: May 28, 2009 Review/Revision Date: December 10, 2012 Next review date: December 10, 2015</p> |
|---|--|