Name of Policy: **Information security framework.**

[redacted]

- 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 [redacted] successful and effective risk management program that continuously evolves and responds to changing threats and opportunities.

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 *(c)* Evaluation and assessment

[redacted]

[redacted]

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.

network must be to "deny everything" and allow only specific services [illegible]

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 [illegible]

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

[redacted]

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-

[redacted]

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.

(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

[redacted]

[redacted]

(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