Information Security of University Technology Resources

For Policy Office Use Only		
Date: 10/4/17	**Policy ID:** IRM-004	**Status:** Revising

Contact Office: University Information Security (InfoSec)

Oversight Executive: Chief Information Officer

Applies to: Academic Division, the Medical Center, the College at Wise, and University-Related Foundations.

Reason for Policy:
The University has a highly complex and resource-rich information technology environment upon which there is increasing reliance to provide mission-critical teaching, research, public service, and healthcare functions. In support of the University's Information Technology Security Program's framework for safeguarding the institution's computing assets in the face of growing security threats, effective security practices are necessary to protect the University's computing infrastructure.

This policy:
1) Defines requirements for owners and overseers of University information technology resources to take reasonable care to eliminate security vulnerabilities from those resources.

2) Establishes the requirement to report information security incidents to appropriate University officials so proper and timely response procedures can be initiated. Such reporting addresses particularly serious incidents, such as violations of confidentiality or integrity of sensitive University data, in order to:

- document and investigate incidents;
- address in a consistent manner and in accordance with data disclosure notification laws which require that the subject of data (e.g., a patient or research subject, credit cardholder) be informed of the incident;
- mitigate any harmful effects of the incident; and
- identify and implement measures to prevent recurrence of the incident.

Reporting also enhances awareness of troublesome trends in security incidents that indicate the need for adjustments in the University's overall security program.

3) Establishes the role of the University Information Security Office and the Health Information and Technology Security Office in monitoring the University's information technology resources for potentially malicious and/or harmful activities and responding to any information security incidents.

4) Establishes the requirement for all departments to participate in the University's Information Security Risk Management Program. The program provides insight into existing risks within a given information technology environment and strategies for reducing or eliminating those risks.

Definitions:
Electronic Device: Electronic equipment, whether owned by the University or an individual, that has a storage device or persistent memory, including, but not limited to: desktop computers, laptops, tablets, smart phones and other mobile devices, as well as servers (including shared drives), printers, copiers, routers, switches, firewall hardware, network-aware devices with embedded electronic systems (i.e., "Internet of things"), and supervisory control and data acquisition (SCADA) and industrial control systems, etc.

Electronic Media: All media, whether owned by the University or an individual, on which electronic data can be stored, including, but not limited to: external hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices (e.g., thumb drives).

Information Security Incident: Any event that, regardless of accidental or malicious cause, results in:
- disclosure of University data to someone unauthorized to access it,
- unauthorized alteration of University data,
- loss of data which the University is legally or contractually bound to protect or which support critical University functions,
- disrupted information technology service, or
- a violation of the University's information security policies.

Examples of such incidents include, but are not limited to:
- Malicious software installations on electronic devices that store University data not routinely made available to the general public, e.g., employee evaluations, or data the University is legally or contractually bound to protect, e.g., social security numbers, credit card numbers, Protected Health Information (PHI), research data, etc.
- Loss or theft of electronic devices, electronic media, or paper records that contain University data not routinely made available to the general public or data the University is legally or contractually bound to protect.
- Defacement of a University website.
- Unauthorized use of a computing account.
- Use of information technology resources for unethical or unlawful purposes (incidents involving employees and pornography should be reported directly to University Human Resources).

- Contact from the FBI, Secret Service, Department of Homeland Security or other law enforcement organizations regarding a University electronic device that may have been used to commit a crime.

Information Technology (IT) Resources: All resources owned, leased, managed, controlled, or contracted by the University involving networking, computing, electronic communication, and the management and storage of electronic data regardless of the source of funds including, but not limited to:

- Networks (virtual and physical), networking equipment, and associated wiring including, but not limited to: gateways, routers, switches, wireless access points, concentrators, firewalls, and Internet-protocol telephony devices;
- Electronic devices containing computer processors including, but not limited to: computers, laptops, desktops, servers (virtual or physical), smart phones, tablets, digital assistants, printers, copiers, network-aware devices with embedded electronic systems (i.e., "Internet of things"), and supervisory control and data acquisition (SCADA) and industrial control systems;
- Electronic data storage devices including, but not limited to: hard drives, solid state drives, optical disks (e.g., CDs, DVDs), thumb drives, and magnetic tape;
- Software including, but not limited to: applications, databases, content management systems, web services, and print services;
- Electronic data in transmission and at rest;
- Network and communications access and associated privileges; and
- Account access and associated privileges to any other IT resource.

Risk Management: The process to identify, control and manage the impact of potential harmful events, commensurate with the value of the protected assets. Risk management includes impact analysis, risk assessment, and continuity planning.

User: Everyone who uses University information technology (IT) resources. This includes all account holders and users of University IT resources including, but not limited to: students, applicants, faculty, staff, medical center employees, contractors, foundation employees, guests, and affiliates of any kind.

Policy Statement:

Owners and overseers of the University's information technology (IT) resources must take reasonable care to eliminate security vulnerabilities from those resources. In cases where University IT resources and privileges are threatened by other IT resources, Information Technology Services (ITS) and Health Information and Technology (Health IT) may act on behalf of the University to eliminate the threat by working with the relevant owners or overseers. In circumstances where these collaborative efforts fail or there is an urgent situation

requiring immediate action, the IT resource may be disabled or disconnected from the network by ITS or Health IT (depending upon the location of the IT resource). This policy applies to all users of the University's information technology resources, regardless of location or affiliation.

All users of University IT resources are required to promptly report information security incidents to appropriate University officials using the procedures at the *Report an Information Security Incident* web page.

Individuals or departments may not release University information, electronic devices or electronic media to any outside entity, including law enforcement organizations, before making the notifications required by this policy.

The University Information Security and the Health IT Security offices are responsible for responding to information security incidents. In addition to following up on reported incidents, these offices may monitor IT resources for potentially malicious and/or harmful activity and take action deemed necessary based on detected activity or in order to enforce a University policy.

The management of each University department or unit is required to complete the process outlined in the *Information Security Risk Management Standard* and *Information Security Risk Management Procedures* at least annually, when there are significant changes to departmental or unit IT resources, or when there are significant changes to the risk environment. The department or unit head will sign off on the deliverables from this process, which will be stored in the University's central repository for these documents.

Compliance with Policy:
Any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this policy and/or its standards may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may also violate federal, state, or local laws.

Questions about this policy should be directed to the Contact Office.

Procedures:
Links will be provided to Standards, Procedures and Guidelines webpages.

Related Information:
In addition to being a widely accepted effective security practice, IT security risk management is required by state and federal regulations. See:

Gramm-Leach-Bliley Act of 1999, Standards for Safeguarding Customer Information; Final Rule – http://www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule

Health Insurance Portability and Accountability Act of 1996 Health Insurance Reform: Security Standards; Final Rule – http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

GOV-002, Reporting Fraudulent Transactions
FIN-037, Governance and Compliance Requirements for Payment Card Activities

Background:

Supersedes (previous policies):
IRM-003: Information Technology Security Risk Management Program
IRM-012: Information Security Incident Reporting
Security of Networked Devices
