University of Massachusetts Medical School
UMASS
The academic partner of UMass Memorial Health Care

Information Security Policy

Policy Number 07.01.11

Effective Date Tuesday, July 31, 2018

Volume VII: Information Technology

Last Revised Tuesday, July 31, 2018

Last Reviewed Monday, March 30, 2020

Responsible Office

» **Policy Administrator** Information Security Officer

» **Contact** 508-856-8643

Policy Statement

The University of Massachusetts Medical School (UMMS) Information Security Policy provides direction for managing and protecting the confidentiality, integrity and availability of UMMS's information assets as defined by NIST 800-53. UMMS is committed to protecting the information that is critical to teaching, research, the Medical School's many varied activities, our business operation (Commonwealth Medicine), and the communities we support, including students, faculty, staff members, and the public. These protections may be governed by legal, contractual, or University policy considerations.

Everyone at UMMS has a responsibility for proper handling and protection of Sensitive information as defined in this Policy. This Policy applies to the entire UMMS community including faculty, staff, contractors and students and pertains to all data types whether electronic or physical. Each policy is supported by Standards that describe what must be done to be compliant. UMMS reserves the right to monitor all systems that are the property of the Medical School or that are attached UMMS network.

Reason for Policy

The purpose of the Information Security Policy is to:

» Provide direction for the confidentiality, integrity and availability of information accessed, held or transmitted in all mediums;

» Define the Medical School's approach and framework for protecting information; »

Provide clear guidance so users may comply with this policy.

Entities Affected By This Policy

This Policy applies to all users including faculty, staff, students, employees, contractors and any other individuals with access to UMMS data or systems.

Related Documents

Additional Information

The following references were used in development of these requirements:

ISO: International Standards Organization

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

NIST: National Institute of Standards and Technology 800-53, 800-88, 800-171

HIPAA: Health Insurance Portability and Accountability Act for protection and confidentiality handling of health information. HIPAA, HITECH, PHI and PII definitions are included on our website:

Executive Order 504: Executive Order regarding security and confidentiality of personal information.

Family Educational Rights and Privacy Act (FERPA): The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Mass. Gen. L. 93H: Commonwealth of Massachusetts Law that protects residents' personal information.

Scope

All individuals that access UMMS resources must adhere to the standards detailed in this document, except where such adherence would conflict with Federal and State laws, regulations or policies. This policy is established to protect the assets and interests of UMMS, to increase overall information security awareness and to ensure a coordinated approach for implementing, managing and maintaining a secure environment.

Responsibilities

The UMMS Information Security Officer (ISO) is responsible for the following:

» Coordinating and overseeing compliance with the Information Security Policy.

» Ensuring the confidentiality, integrity and availability of UMMS's information technology resources and data by safeguarding them from compromise, misuse, loss or damage (intentionally and unintentionally) allowing UMMS to continue its mission critical operations of education, research, service and administration.

» Working closely with the Chief Information Officer (CIO) to develop, implement and ensure compliance with policies, standards and procedures related to the security of UMMS information.

» Ensuring that information Security policies, standards and procedures are reviewed with Medical School stakeholders through various committees and other governing bodies.

» Lead the Information Security Incident Response Team (SIRT). The SIRT team is comprised of individuals with decision-making authority from within the Medical School and charged by Senior Management the responsibility of coordinating and overseeing the response to incidents in accordance with the requirements of state and federal laws and University policy.

» Conduct appropriate due diligence to ensure that third-parties that store or have access to UMMS Sensitive information are capable of properly protecting that information.

» Oversee information security awareness and training programs for the Medical School.

» Monitor the UMMS network and systems to ensure that threats are identified and mitigated.

» Provide regular Information Security threat and risk updates to Medical School Senior Management.

The UMMS Senior Privacy Officer is responsible for the following:

» Developing and implementing policies and procedures governing the privacy of UMMS data, including data entrusted to us from our partners.

» Ensure that research data complies with relevant regulatory requirements.

» Oversee privacy awareness and training programs for the Medical School.

UMMS Managers and Supervisors are responsible for the following:

» Ensuring information security policies, standards and procedures are followed by employees in their respective areas.

» Ensuring that all individuals within their charge take annual information security and privacy training.

» Ensure that information security and privacy requirements are topics in regular staff meetings.

» That UMMS data access within their respective areas is appropriate and reviewed regularly.

All users with physical or logical access to UMMS data or systems are responsible for the following:

» Protecting Sensitive information in any form from unauthorized access and use.
» Protecting passwords and other access credentials from unauthorized use.
» Using Sensitive information for authorized purposes exclusively.
» Participate in required annual information security and privacy training.
» Only accessing information resources through approved UMMS accounts.
» Only accessing information resources through approved computers, laptops or portable devices.
» Appropriately protect electronic and physical records containing Sensitive information in transport or during transmission.
» Ensuring that computers used to access Sensitive information are encrypted.
» Securely dispose of electronic and physical records containing Sensitive information when no longer needed or required so that the information cannot be retrieved or reassembled.
» Reporting any actual or suspected loss, theft, or improper use of or access to Sensitive information.
» Complying with this policy, and all UMMS policies, standards and procedures.

The UMMS Information Technology Department is responsible for the following:

» Ensuring software is kept up to date and security patches applied on all computers and devices.
» Ensuring there is a mechanism to limit the number of unsuccessful attempts to log into an application or server that processes or stores UMMS information.
» Ensuring that all servers storing UMMS are protected against improper or unauthorized access.
» Ensuring that all systems where information is stored must be accurately identified and physically secure.
» Ensuring that capabilities to encrypt data at rest and in transit are available for those systems where required.

Definitions

Sensitive data – Data containing PII, PHI, individually identifiable medical records and genetic information, human resource information, specific contractual or customer obligations and research information.

Users – Any individual with logical or physical access to UMMS systems or data.

Compliance and Enforcement

Any UMMS user violating any provision or portion of this policy may be denied access to UMMS systems or data and may be subject to disciplinary action, up to and including dismissal from a School or termination of employment.