University of Massachusetts UMASS Medical School
The academic partner of UMass Memorial Health Care
(http://www.umassmed.edu/)

Encryption

Volume VII: Information Technology
Policy Number 07.01.06
Effective Date Saturday, August 01, 2015
Last Revised Thursday, November 17, 2016
Last Reviewed Monday, March 08, 2021

Responsible Office

- **Policy Administrator** Information Security Officer
- **Contact** 508-856-8643

Policy Statement

Schools, departments and business functions are required to apply University-approved encryption solutions to preserve the confidentiality and integrity of, and control accessibility to, University of Massachusetts Medical School (UMMS) data classified as Highly Restricted or Confidential* where this data is processed, stored or transmitted.

** Refers to Data Classification policy 07.01.03*

Reason for Policy

The purpose of this policy is to establish: the types of data, devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software and techniques used for encryption.

Entities Affected By This Policy

This policy affects all department heads, chairs, faculty and staff responsible for ownership or oversight of UMMS data, as defined by the Data Classification Policy.

Related Documents

- Data Classification Policy
- Acceptable Use Policy

Scope

University Information is any information maintained by or on behalf of the University that is used in the conduct of University business, regardless of the manner in which such information is maintained or transmitted. University Information formats include, but are not limited to, oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

Responsibilities

Users who work with UMMS data must encrypt their data to prevent unauthorized disclosure.

Researchers who work with UMMS data approved by their respective IRB must encrypt their data to prevent unauthorized disclosure.

Procedures

- All databases that contain UMMS Highly Restricted or Confidential data must encrypt the data at rest, with the exception of those University resources housed in approved restricted-access facilities such as UMMS data centers.
  - If there are contractual requirements for data at rest, data must be encrypted.

- All databases, application servers and file systems that contain UMMS Highly Restricted or Confidential data must leverage appropriate network access controls to ensure that access to the data is limited to those whose job functions require access.

- Servers must not be directly accessible from the Internet or from publicly facing servers of the UMMS networks unless the information is encrypted.
  - Information may be accessed remotely through an approved VPN connection. The use of an approved VPN is not considered direct access.
  - UMMS Highly Restricted and Confidential Information must be encrypted when it traverses any network outside of the UMMS network.

- Encryption is required for all laptops, workstations, mobile devices and portable drives that may be used to store or access UMMS data.
  - Laptops and Desktops that access third-party data (i.e., UMMHC) must comply with all data protection and encryption policies of the third-party.
  - Departments who have a laptop, workstation, mobile device, or portable drive that needs to be encrypted must contact the UMMS Information Technology Help Desk.

- All electronic messages containing UMMS Highly Restricted or Confidential data that are transmitted to any entity, institution, or group outside of the UMMS secured network must apply appropriate levels of encryption.
  - Portal-based encryptions Transport Layer Security (TLS) and Secure File Transfer Protocol (SFTP) are acceptable encryption methods for message transmission.

- Backups that contain UMMS Highly Restricted or Confidential data must be encrypted when stored outside of secured, primary locations.
- Information can be stored on external devices with specific requirement and approval:
  - All portable media (including portal disk or thumb drives) containing UMMS Highly Restricted or Confidential data must be encrypted and a list of individuals with access to the media must be provided.
  - The device must be stored in a locked container when left unattended.
  - Whole disk encryption services are available for both Windows and Macintosh desktop and laptop computers as well as mobile devices such as external hard/flash drives.

Definitions

Encryption is the conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized individuals. Encryption is a very important tool to safeguard protected and confidential data, but it is a powerful tool that needs to be installed and used with caution.