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

Acceptable Use Policy

Policy Number 07.01.01

Effective Date Wednesday, December 31, 2014

Volume VII: Information Technology

Last Revised Thursday, June 21, 2018

Last Reviewed Monday, March 30, 2020

Responsible Office

» **Policy Administrator** Information Security Officer

» **Contact** 508-856-8643

Policy Statement

It is the policy of the University of Massachusetts Medical School (UMMS) to encourage widespread access and distribution of data and information. UMMS maintains access for its community to local, national, and international sources of information and provides an atmosphere that encourages the free exchange of ideas and sharing of information. Access to this environment and the UMMS information technology resources is a privilege and must be treated with the highest standard of ethics.

UMMS expects all members of the community to use computing, data, and information technology resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and UMMS policies and standards.

Reason for Policy

UMMS has an obligation to protect the integrity of information technology resources, the rights of all users and the property of the UMMS in its sole discretion. **UMMS thus, reserves the right to examine material stored on or transmitted through its resources if there is cause to believe that the standards for acceptable and ethical use are violated** by a member of the UMMS community or a trespasser onto its systems or networks.

UMMS reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other UMMS-owned computing device, to monitor, to seize such device and/or copy or have copied and/or wipe or have wiped, any and all information from the data storage mechanisms of such device as may be required in the sole discretion of UMMS in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the University network are also subject to inspection and/or monitoring by authorized University personnel. **Information Disclaimer**

Individuals using computer systems owned by the University do so subject to applicable laws and UMMS policies. UMMS disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the Commonwealth of Massachusetts, the University, its faculty, staff, or students.

I have read and agree to abide by the entire content of this Acceptable Use Policy and all related policies/guidelines/standards referenced herein. I recognize my overall responsibility to exercise the degree of care required to maintain control of University computing systems and resources (e.g. data, software, hardware, network components, etc.) and agree to abide by established University policies/guidelines/standards and College procedures. I acknowledge that failure to comply with University Acceptable Use related policies/guidelines/standards/procedures might result in: the loss or restriction of my computer access; reprimand, suspension; dismissal, or other disciplinary or legal action.

Print Name:_____

Signature:_____ Date:_____

NOTICE OF RIGHT TO CHANGE ACCEPTABLE USE POLICY

UMMS reserves the right to change this policy or any portion of the policy, at any time, with or without prior notice. The AUP was last revised on June 21st, 2018

Entities Affected By This Policy

This policy applies to all users of computing, data, and information technology resources including faculty, staff, students, guests, external organizations and individuals accessing network services, such as the Internet, via UMMS resources. By accessing and/or using University information systems, and/or by "clicking through" a usage agreement during UMMS or other equipment registration procedure, users assent to the Terms and Conditions of the Acceptable Use Policy.

Preserving access to information resources is a community effort that requires each member to act responsibly and guard against abuses or negligence. Therefore, both the community as a whole and each individual user have an obligation to abide by and hereby agree to the **following standards of acceptable and ethical use.**

Related Documents

Data Classification Policy (/Policies/Policies-listing-page/it/Data-Classification/) Encryption

Policy (/Policies/Policies-listing-page/it/encryption/)

Scope

This policy outlines the standards for acceptable use of UMMS computing, data, and information technology resources, which include, but are not limited to, equipment, software, networks, data, and telephones whether owned, leased, transmitted across, or otherwise provided by the Office of Information Technologies at UMMS.

Responsibilities

Enforcement and Monitoring

UMMS considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to monitor, to copy and/or examine any activity, files or information resident on UMMS systems allegedly related to unacceptable use and to protect its network from systems and events that inappropriately expose data or information or threaten or degrade operations. Violators are subject to disciplinary action as prescribed in the UMMS Code of Conduct and employee handbooks. Offenders also may be prosecuted under applicable federal and state law.

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information property, and may subject the University to penalties and the user to discipline.

Any member of the UMMS community found using information resources for unethical and/or unacceptable practices is in violation of this policy and may be subject to disciplinary proceedings including suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate.

UMMS reserves the right to limit or restrict the use of its computing and information technology resources based on institutional priorities and financial considerations. Further it may restrict access based on evidence of a violation of University policies, contractual agreements, or state and federal laws.

Procedures

Acceptable and Ethical Use:

1.1 Complete all privacy and security training required of your position in a timely manner.

1.2 Use UMMS resources only for authorized purposes, including limited personal use. Exercise good judgment regarding the reasonableness of personal use.

1.3 Conduct all communication, including electronic, in a responsible manner. This includes safeguarding the integrity and confidentiality of University electronic communication (e.g. email).

1.4 You are responsible for all activities which originate from your user ID or from your assigned computing device. Access only your own information, or information that is publicly available, or to which you have been granted access.

1.5 Use only those computing, data and information technology resources for which you have authorization and only for their intended purpose.

1.6 Protect the access to and integrity of computing, data, and information technology resources.

1.7 Ensure that sensitive data is created, collected, maintained, used, disseminated, and destroyed in a manner that prevents unauthorized use, corruption, disclosure, loss or theft accordingly to UMMS policy, legal and contractual requirements.

1.8 Properly create, collect, maintain, access, disseminate and dispose of University data based on the data's classification to prevent unauthorized use, corruption, disclosure, loss or theft accordingly to UMMS policy, legal and contractual requirements.

1.9 Abide by applicable laws and UMMS policies and respect the copyright and intellectual property rights of others, including the legal use of copyrighted software. Illegal distribution of copyright software within or outside of the University through any mechanism, electronic or otherwise, is strictly prohibited.

1.10 Respect the privacy and personal rights of others. For example, do not rebroadcast or forward information obtained from another individual that the individual reasonably expects to be confidential, except as required by your job responsibilities, University Policy and applicable laws.

1.11 Internet use must comply with the Terms of Service stipulated by our Internet service provider(s).

1.12 Never use UMMS resources to engage in any illegal activity.

1.13 Immediately report compromises and other security incidents to the Information Technology Help Desk, including but not limited to, the loss or theft of portable/mobile devices.

1.14 Encrypt data in compliance with UMMS policy and in accordance with applicable state and federal regulations.

The following activities, while not an exhaustive list, are examples of unacceptable use and are PROHIBITED:

1.16 Use of another person's account, identity, security devices/tokens, or presentment of false or misleading information or credentials, or unauthorized use of information systems/services.

1.17 Share account credentials (username / password) with anyone.

1.18 Access and/or disclose confidential or sensitive data or sensitive system or network information except as authorized as part of your duties and according to established standards.

1.19 Access or use data or information unless you are authorized to do so.

1.20 Distribute information that violates existing laws, or University policy, procedures, and code of conduct.

1.21 Remove or delete data (e.g. email), including from a remote location, unless required for job responsibilities and in a manner consistent with record retention requirements.

1.22 Use computer programs to decode passwords, access control information, send chain emails, spam, generating excessive printing and other inappropriate behavior.

1.23 Use of systems to harass, threaten, libel or defame any person.

1.24 Attempt to circumvent or subvert system and network security measures.

1.25 Operate any UMMS system or any system on the UMMS network without the use of Anti-Virus software configured to auto-update.

1.26 Engage in any activity that may be purposely harmful to UMMS data, systems or networks.

1.27 Use UMMS systems or networks for commercial or political purposes (unless otherwise specified in the IP agreement).

1.28 Use UMMS systems or networks to conduct activities that pose security risks. Sites that offer gambling, adult content or cryptocurrency often contain malicious content and should be avoided .

1.29 Make illegal copies of copyrighted materials or software, photograph or capture images of protected information.

1.30 Use the UMMS systems or networks for personal gain, profit or convenience (unless otherwise specified in the IP agreement)

1.31 Connect unauthorized equipment (for example, a personal wireless access point) to the UMMS network, directly or via remote connection.

1.32 Visit internet sites that contain illegal content.

1.33 Abuse highly-authorized or administrative privileges to access data or systems unnecessarily or inappropriately.

Definitions

Data Encryption – The process of converting unencrypted plain text into encrypted cyphertext, which maintains data privacy even if the data are lost or stolen.

Mobile Code – Software that resides on a website, which moves to a user's computer and runs within the user's web browser. Examples include Java, ActiveX, Visual Basic (VB script)

PHI – Protected Health Information

PII – Personally Identifiable Information

Portable Media -- All portable devices which can store electronic data including but not limited to laptop computers, portable disk drives, CD and DVD media, backup tapes, cellular telephones, PDAs, audio recorders, and thumb drives

UMMS – University of Massachusetts Medical School

UMMSNet – University of Massachusetts Medical School's computing resources

UMnetID – User credentials (username/password) pertaining to centralized Active Directory account.