University of
Massachusetts
UMASS Medical School

UMASS MEDICAL SCHOOL IT INFORMATION TECHNOLOGY

SECURITY INCIDENT REPORTING PROCEDURES

ⓘ Report all suspected or confirmed Security Incidents Immediately!

The University of Massachusetts Medical School (UMMS) Information Security (IT) Help Desk *(508) 856-8643* should be notified immediately of any suspected or confirmed Security Incident involving UMMS Technology Assets or UMMS information in electronic or hardcopy format.

A UMMS Information Technology Asset includes any system or systems that process, stores or transmits UMMS information. This includes hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, laptops, mobile devices, servers, printers, telephones, network lines, E-mail and web based services. Hardcopy data which includes sensitive or protected information must also be reported if lost or stolen.

Security Incident – an incident meeting one or more of the following conditions:

- Any potential violation of Federal law, Massachusetts law or UMMS Policy involving a UMMS Information Technology Asset or sensitive or protected information in any form
- A breach, attempted breach or other Unauthorized Access of a UMMS Information Technology Asset. The incident may originate from the UMMS network or an outside entity and generate from the following:
  - External/Removable Media: An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
  - Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services
  - Web: An attack executed from a website or web-based application.
  - Email: An attack executed via an email message or attachment.
  - Improper Usage: Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- Any Internet worms or viruses
- Any conduct using in whole or in part a UMMS Information Technology Asset which could be construed as harassing, or in violation of UMMS Policies
- The loss or theft of a UMMS computing device (including desktop, laptop computers and mobile devices) or the loss of any personal computing device containing UMMS information

Unauthorized Access - Any action or attempt to utilize, alter or degrade a UMMS owned or operated Information Technology Resource in a manner inconsistent with UMMS policies.

University of Massachusetts
UMASS Medical School

UMASS MEDICAL SCHOOL IT INFORMATION TECHNOLOGY

Reporting a Security Incident:

UMMS IT Help Desk staff should be notified immediately of any suspected or confirmed Security Incident involving a UMMS Information Technology Asset. If after normal operating hours, UMMS Campus Police should be notified (number). If it is unclear as to whether a situation should be considered a Security Incident, UMMS Information Security staff may be contacted to evaluate the situation.

Special Consideration for Lost or Stolen Computing Devices:

In the event that a UMMS computing device (including mobile devices such as laptops and smart phones) or personal device containing UMMS information is lost or stolen UMMS Campus Police should be notified immediately. Campus Police will bring in UMMS Information Security to assist in required investigation and forensics activity.

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by IT Information Security personnel. When faced with a potential situation involving a suspected or actual breach or virus or malware infiltration, UMMS faculty and staff should do the following:

- If the incident involves a compromised computer system, do not alter the state of the computer system. The computer system should remain on, and all currently running computer programs should be left as is. Do not shutdown the computer or restart the computer.
- Immediately disconnect the computer from the network by removing the network cable from the back of the computer.
- Report the security incident.

Security Incidents involving possible violation of Federal or state law should be immediately reported to the UMMS Campus Police. UMMS Campus Police will work with IT Information Security staff and other law enforcement agencies as necessary to help resolve the incident.

IT Information Security staff will first determine if the Security Incident justifies a formal incident response. In cases where a Security Incident does not require an incident response, the situation will be forwarded to the appropriate area of IT to ensure that all technology support services required are rendered.

An incident response may range from getting a critical system back online, gathering evidence, taking appropriate legal action against individual(s), or in some cases notifying appropriate ISP's or other third parties of inappropriate activity originating from their network.