Policy Title: IT6004 - Security and Protection of Electronic Information Resources

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

The University of Memphis (UofM) has established and maintains an array of information technology resources (e.g. software and systems, networks, servers, pc's, printers and other devices) collectively known as the University of Memphis "IT Commons." This IT Commons exists to serve the needs of the faculty, staff, and students at the UofM. The UofM communication networks are a critical component of the IT Commons.

Access to UofM technology resources is a privilege, not a guarantee, and may be revoked at any time for violation of acceptable use (see policy IT6003 - Acceptable Use of Information Technology Resources.)

The University requires that all equipment that attaches to the UofM network meets certain minimum standards to assure the operational integrity and security of the UofM IT Commons. Any equipment, including virtual devices, that fails to meet minimum required standards for operational integrity and security are subject to removal from the network unless an exception is granted by the Chief Information Officer (CIO).

Each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control over. Resources to be protected include networks, devices, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

This policy defines procedures for the security and protection of university electronic information resources, as well as, to define security action processes during a state of emergency.

Procedures

Detection and Prevention

Information Technology Services (ITS) is responsible for operating and managing campus communications networks as a campus resource available to all members of the campus community. ITS is authorized to monitor network activity and usage as necessary to detect potential network abuse or threats to the availability or integrity of campus information resources. Upon detecting a security breach, ITS, in consultation with the Office of Legal Counsel, shall exercise due diligence in the timely investigation of suspected security incidents and promptly communicate with Local Support Providers (LSPs) and other campus users regarding actions that may be required to protect campus information resources.

To prevent security breaches, LSPs have an ongoing responsibility:

- to work closely with ITS staff to securely and consistently maintain and support IT commons.
- to be knowledgeable of relevant security threats and remediation strategies.
- to analyze potential or actual threats to their business units.
- to put in place security measures that protect their business units.

to provide recommendations to appropriate ITS officials.

Response to Threats to the IT Commons

The Chief Information Officer (CIO), or designee, in consultation with the Office of Legal Counsel, has the authority to limit and/or suspend network privileges of individuals or systems to halt any activities that adversely disrupt network services or that create security incidents as defined by relevant laws and University policy. This authority includes temporary isolation of systems or devices from the network and revocation of network privileges of individuals without advance notice.

The CIO, or designee, has the authority to evaluate the seriousness and immediacy of any threat to campus information system resources or the Internet and to take necessary action to mitigate that threat. Actions taken will be responsible and prudent based on the risk associated with that threat and the potential negative impact to the campus IT Commons.

IT State of Emergency

In the event of an actual attack on the network, or a credible warning of an impending attack, the university's CIO will mobilize all available resources, including LSPs, to counter the attack and/or threat, or to recover from an attack. The CIO will determine if an attack/threat rises to the level of a "state of emergency." During a declared IT State of Emergency, ITS will provide

leadership and supervision for all ITS and LSP personnel until the attack/threat has been eliminated and the network has been restored to normal operations.

Once an IT State of Emergency is declared, and for its duration, the CIO will review the situation with the President and executive staff, and provide regular, periodic briefings on status.

After an IT State of Emergency ceases, the CIO will prepare an impact report for the President and executive staff.

Local Support Provider Responsibilities During a Declared IT State of Emergency

For the duration of any declared IT State of Emergency, all LSPs will report operationally to the CIO. These actions are critical to ensure the University's IT Commons is protected and restored as quickly as possible to normal operations.

LSPs will

- as directed by ITS, implement security measures to mitigate threats
- follow the directives of designated ITS staff during the declared state of emergency

ITS will assign campus IT staff resources (LSPs as well as ITS Staff) to priorities of greatest need. In all cases, ITS will task LSP staff to respond to the needs of their home department/units as quickly as possible.

FAQs

What are examples of threats serious enough to invoke a Declaration of an IT State of Emergency?

- Levels of illicit network activity cause serious degradation in the performance of the network.
- System administrative privileges have been acquired by an unauthorized individual(s).
- An attack on UofM computers or the network has been launched, or UofM staff has reason to believe such an attack is imminent.
- Unauthorized capture of confidential, private or proprietary electronic information or communications has been detected.
- UofM receives external reports of illegal, illicit activities emanating from UofM that are threatening other networks.

Related Documents, Policies and Forms

IT6003 - Acceptable Use of Information Technology Resources

GE2008 - Crisis Management Planning

Last Revision Update Log: 12/15/2022

IT6004 – Revised March 27, 2018
IT6004 – Revised March 14, 2019
IT6004 – Revised March 27, 2018 – supersedes policy number
UM1566 – Revised: May 09, 2014
UM1566 – Issued: January 25, 2008