Texas A&M Health Science Center Guidelines

29.01.03.Z1.19 Guideline: Malicious Code

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01.03 and TAMU SAP 29.01.03.M1.23

Reason for the Guidelines

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. This guideline applies equally to all individuals who use any Texas A&M University Health Science Center (HSC) information resource.

1. Malicious Code

1.1 All personal computers whether connected to the HSC network, or university owned standalone, must use the HSC Office of Information Technology (OIT) approved malware protection software and configuration, if practical.

1.2 The malware protection software must not be disabled or bypassed.

1.3 The settings for the malware protection software must not be altered in a manner that will reduce the effectiveness of the software.

1.4 The automatic update frequency of the malware protection software must not be altered to reduce the frequency of updates.

1.5 Each file server attached to the HSC network must utilize HSC OIT approved malware protection software unless there is a demonstrated technical justification for an exception and the exception is documented and approved as a risk management decision.

1.6 Each E-mail gateway must utilize HSC OIT approved e-mail malware protection software and must adhere to the OIT rules for the setup and use of this software.

1.7 Malicious code that is not automatically cleaned by the malware protection software constitutes a security incident and must be reported to OIT.
2. Violations

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration