


<b>Name of Policy:</b> <u><a href="#">Malicious code security.</a></u> <b>Policy Number:</b> 3364-65-15 <b>Approving Officer:</b> President <b>Responsible Agent:</b> Vice President of Information Technology <b>Scope:</b> all University campuses		 <b>Original effective date:</b> May 28, 2009	
<input checked="" type="checkbox"/>	New policy proposal	<input type="checkbox"/>	Minor/technical revision of existing policy
<input type="checkbox"/>	Major revision of existing policy	<input type="checkbox"/>	Reaffirmation of existing policy

(A) Policy statement

The University of Toledo will ensure that university-controlled computer systems are suitably protected from malicious code exploits through the implementation of a malicious code security program.

(B) Purpose

Computer viruses and other forms of malicious code are constantly being developed and transmitted via many methods to unsuspecting computer users around the world. This policy requires the IT department to develop and implement a malicious code security program which all university organizations must adopt. The program is intended to ensure that adequate protective measures are in place against the introduction of malicious code into university-controlled information systems, the detection of such code should it become resident in computing systems, and that computer system users are able to maintain a high degree of malicious code awareness.

(C) Scope

The scope of this information technology policy includes university computer and telecommunications systems, non-university owned systems that are connected to the university's internal network, and the employees, students, contractors, temporary personnel and other agents of the university who use and administer such systems.

(D) Requirements

(1) Malicious code security capability. The university shall acquire and deploy appropriate malicious code security. At a minimum, the following shall be accomplished:

(a) Software designed to detect and prevent the installation of malicious code shall be provided for university-owned systems.

(b) Organizations that maintain computing systems are expected to:

(i) Know the current requirements.

- (ii) Have security software installed that meets the requirements.
  - (iii) Keep their systems current and patched.
  - (iv) Report to IT security when systems have been compromised by malicious code.
- (2) Individual responsibilities. Each employee, student, contractor, temporary worker or other agent of the university who operates a privately-owned desktop or laptop computer that connects to the university's internal network shall:
- (a) Have current anti-virus software installed and operating with up to date anti-virus signatures.
  - (b) Keep their systems current and patched including operating systems and installed applications.
  - (c) Upon determining that a computer has been compromised, immediately disconnect it from the university's network.
  - (d) Report to IT security when their system has been compromised by malicious code while connected to the university's internal network.
- (3) Malicious code education and awareness.
- (a) Information technology shall establish malicious code security education and awareness efforts in accordance with university policy for "Security Education and Awareness." At a minimum this training shall include instructional materials for malicious code security as described throughout this policy.
- (4) Procurement. Organizations shall ensure that procurement processes contain assurances, including but not limited to contract terms, that any software or other deliverables are free from known malicious code.

(E) Definitions:

- (1) Anti-virus software. A commercially available computer program that detects, contains and eradicates malicious code.
- (2) Computer virus. A small, self-replicating, malicious program that attaches itself to an executable file or an application and executes commands that can range from annoying to extremely destructive.
- (3) Malicious code. Collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>June 11, 2009</u> Date</p> <p>Review/Revision Completed by: <i>Vice President of Information Technology</i></p>	<p>Policies Superseded by This Policy:</p> <p>None</p> <p>Initial effective date: May 28, 2009</p> <p>Review/Revision Date: Next review date: May 28, 2011</p>
---	--