Ohio Supercomputer Center Malicious Code Security	**No:** **OSC-4**
	Effective: **05/21/09**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

This policy is to implement and operate a ***malicious code*** security program. The program should help to ensure that adequate protective measures are in place against introduction of malicious code into OSC information systems and that computer system ***users*** are able to maintain a high degree of malicious code awareness.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this policy applies to all systems under the control of the Ohio Supercomputer Center.

The scope of this information technology policy includes OSC computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

3.0 Background

Computer viruses and other forms of malicious code are constantly being developed and transmitted via many methods to unsuspecting computer users around the world. The purpose of this policy is to ensure that OSC ***system assets*** are suitably protected. This can be accomplished by an appropriate mix of preventive measures, including policy, ***anti-virus software***, and education and awareness programs.

4.0 References

4.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state chief information officer to establish State of Ohio IT policies as they relate to state agencies' acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.

4.2 Ohio IT Policy ITP-B.1, "Information Security Framework," is the overarching umbrella security policy for state information and services. Ohio IT Policy ITP-B.4, "Malicious

Code Security," is one of several sub-policies. These security policies should be considered collectively rather than as separate or unrelated policies. Attachment 1 illustrates the interrelationship of state technology security policies.

4.3 Ohio IT Policy ITP-B.7, "Security Incident Response," requires the state and its agencies to develop and maintain an adequate security response capability for identified security incidents.

4.4 Ohio IT Policy ITP-B.8, "Security Education and Awareness," requires state agencies to provide information technology security education and awareness to employees and other agents of the state.

4.5 A glossary of terms found in this policy is located in section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

5.0 Policy

This malicious code security policy is in compliance with the statewide policy and ensures that all users of OSC controlled systems adhere to at a minimum, the following requirements:

5.1 Malicious Code Security Capability. OSC will follow the Ohio State University procedures and deploy a malicious code security (often referred to as anti-virus) capability. At a minimum, the following shall be accomplished:

5.1.1 Ensure that anti-virus software is installed and operating properly on OSC owned and operated information systems.

5.1.2 The software will check daily for updates to anti-virus software and begin installing all updates immediately. When the anti-virus software developer supplies notification of an update, implementation of that update shall begin immediately.

5.1.3 Scan in real time all e-mail attachments transmitted from both the Internet and intranet for malicious code.

5.1.4 Check all files and attachments from Web sites and ***instant messaging***, including downloaded files, for malicious code.

5.1.5 Check all removable media such as diskettes, USB or CD-ROMs for malicious code before they are used on OSC systems.

.

5.1.6 Ensure that all software, including internally-developed application software, is free from malicious code before installation onto a computer or other system asset.

5.1.7 Check all servers daily for malicious code. For all other system assets check for malicious code weekly, or more frequently commensurate with their risk per the OSC risk assessment.

5.1.8 Ensure that all mainframes and servers connected to PCs for any interface function are protected consistent with this policy.

5.1.9 Designate a point of contact (POC) who will either provide support directly, or who can serve as an intermediary to get support for affected systems.

5.1.10 Establish a procedure for reporting malicious code incidents to the designated POC. The POC shall report the incident in accordance with "OSC Security Incident Response."

5.1.11 Maintain a record of malicious code incidents for auditing purposes.

5.1.12 Establish procedures for resolving malicious code incidents. The procedures shall include consideration of any need to preserve legal evidence.

5.2 Individual Responsibilities. Each employee, contractor, temporary worker or other agent of OSC who operates a privately-owned desktop, laptop computer or Personal Data Device (iPhone, Blackberry, etc) in conjunction with OSC systems is responsible for the following:

5.2.1 Maintaining awareness of malicious code risks and potential for damage.

5.2.2 Not distributing malicious code.

5.2.3 Not disabling anti-virus software.

5.2.4 Reporting any malicious code encountered or other similar activity to the designated POC.

5.2.5 Properly installing and using up-to-date anti-virus software consistent with agency policy and practice with regard to privately-owned computers that the user has permission to use for OSC. Nothing in this policy shall be construed to mean that agencies must grant this permission or be responsible for the installation, maintenance and support of privately-owned computers.

5.3 Malicious Code Education and Awareness.

5.3.1 OSC shall establish malicious code security education and awareness efforts in accordance with Ohio IT Policy ITP-B.8, "Security Education and Awareness." At a minimum this training shall include instructional materials for malicious code security as described throughout this policy.

5.3.2 OSC shall ensure that each employee, contractor, temporary worker or other agent of OSC who uses OSC-controlled systems receives initial, ongoing and refresher training on malicious code security, including how to use the anti-virus software issued by OSC.

5.4 Procurement. Agencies 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.

6.0 Procedures

None.

7.0 Implementation

The policy is in effect beginning with acceptance.

8.0 Revision History

Date	Description of Change
6/1/2009	Original policy.
03/19/2011	Scheduled policy review.

9.0 Definitions

9.1 Anti-Virus Software. A commercially available computer program that detects, contains and eradicates malicious code.

9.2 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.

9.3 Instant Messaging. A software tool that allows real-time electronic messaging or chatting. Instant messaging services use "presence awareness" indicating whether people on one's list of contacts are currently online and available to chat. Examples of instant messaging services are AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.

9.4 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.

9.5 System Assets. Information, hardware, software and services required to support the business of the agency, and identified during the risk assessment process as assets that need to be protected in accordance with Ohio IT Policy ITP-B.1, "Information Security Framework."

9.6 Users. For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned computer and telecommunication systems on behalf of the state.

10.0 Related Resources

None.

11.0 Inquiries

Direct inquiries about this policy to:

Director of Supercomputer Operations
1224 Kinnear Rd.
Columbus, OH 43212

Telephone: 614-292-9248

OSC IT Policies can be found on the Internet at: www.osc.edu/policies