OhioDAS

INFORMATION SECURITY AND PRIVACY POLICY
MALICIOUS CODE DEFENSE

IT POLICY NUMBER: 2100-03

EFFECTIVE DATE: 12/05/2012

APPROVED BY: _____

Robert Blair, Director
Department of Administrative Services

1.0 PURPOSE

This policy addresses the prevention, detection, removal, and reporting of malicious software; for example viruses, logic bombs, Trojan horses, worms, key loggers, and spyware; which may impact IT resources owned, managed, or operated by the Department of Administrative Services (DAS). The goal is to assure that proactive security measures are taken to prevent malicious software attacks from occurring; to raise awareness for recognizing and immediately reporting the occurrence of malicious software; and to ensure that appropriate action is taken to minimize the consequences of a malicious software attack.

2.0 SCOPE

This policy applies to computer and telecommunications systems owned or operated by DAS and the managers of DAS business units and IT systems that use or 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. This policy is intended to ensure that DAS' IT resources are suitably protected from malicious software. Protection against malicious code includes an appropriate mix of preventive measures including enforceable policy, anti-malware software, education and awareness, and network and system monitoring.

4.0 REFERENCES

4.1. **Ohio IT Standard; ITS-SEC-02; Security Controls Framework:** This state IT standard specifies the minimum requirements for information security in all ***agencies*** and identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53, revision 3 (NIST 800-53) as the framework for information security controls implementation for the state.

4.2. **NIST Special Publication 800-53 (Rev 3),** ***Recommended Security Controls for Federal Information Systems and Organizations***, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

4.3. **DAS Policy; 700-01, IT Resource Usage:** This DAS policy establishes controls on the use of IT resources in accordance with Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources."

4.4. **DAS Policy; 2100-02, Mobile Computing:** This DAS policy establishes controls on the use of portable computing devices and remote access.

4.5. **DAS Procedure; Incident Response:** This DAS procedure defines the steps to follow for DAS' response to any type of critical incident, including security incidents, that affects DAS' applications, systems, networks, infrastructure or capability to deliver services.

4.6. A glossary of terms found in this policy is included in Section **8.0 – Definitions**.

5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS' IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

DAS Programs shall implement appropriate malicious code security practices in compliance with this policy and ensure that users of DAS controlled systems adhere to this policy.

5.1 Malicious Code Security Capability

DAS Programs shall acquire and deploy capabilities which will manage and reduce risk due to malicious code on all systems owned or operated by DAS. As a minimum, all of the following shall be accomplished.

Prevention

5.1.1. Anti-malware software shall be installed and operating properly on DAS owned, operated, or authorized system assets whenever possible.

5.1.2. Daily checks for updates to anti-malware software and virus definition data shall be performed. Available updates shall be installed within twenty-four hours of availability from the manufacturer. If feasible, available updates shall be installed immediately.

5.1.3. Upon notification of a new or emerging malicious code threat, DAS shall inquire with the manufacturer about the availability of definition updates and/or system patches and obtain/deploy them as soon as the update or patch becomes available.

Detection

5.1.4. DAS shall use anti-malware software to scan in real-time all incoming and outgoing e-mail messages, attachments, and files for viruses and other malicious software. Malicious code shall be quarantined or deleted before allowing the e-mail to be delivered.

5.1.5. Technology shall be implemented to check all files and attachments from websites and instant messaging, including downloaded files, for the presence of malicious code. File downloads from un-trusted websites should be limited unless necessary to support DAS business operations. Note that restrictions on instant messaging and file downloading are currently specified in DAS Policy 700-01: IT Resource Usage.

5.1.6. DAS shall implement controls to ensure that removable media such as, diskettes, CD-ROMs, and USB file drives are checked for malicious code before they are used on DAS systems. DAS shall also implement controls to ensure that portable computing devices, such as laptop computers and personal digital assistants (PDAs) are checked for malicious code before they are connected to DAS networks.

5.1.7. The appropriate steps shall be performed to ensure that all software, including internally developed application software, is free from malicious code before installation onto a computer or other device.

5.1.8. When feasible, servers owned or operated by DAS shall be scanned for malicious code at least once daily. A written variance must be obtained and maintained via DAS' Policy Exemption/Deferment Request process for servers for which a different scanning schedule is necessary.

5.1.9. Scans for malicious code shall be performed on all non-server system assets on a schedule commensurate with the system risk level determined by DAS' risk assessment.

Removal

5.1.10. Any device thought to be infected by an unknown virus or other unidentified malicious code with no known cleaning routine available shall immediately be isolated and appropriate measures shall be taken to remove the malicious code. If necessary, the device shall be disconnected from all networks. If the malicious code cannot be removed, the device shall remain disconnected from the network.

5.1.11. Off-the-shelf malware scanning tools shall be used to remove a virus or other malicious code from infected files, programs, or storage media. If scanning tools still do not remove the malicious code and the scanning tool manufacturer cannot provide an update in a satisfactory time-frame, all software on the device shall be deleted including boot records. The software shall then be reinstalled from uninfected sources and rescanned for malicious code. All devices shall be carefully checked for suspected sources and locations of malicious code, including any shared network services, programs, e-mail messages, and files. All devices shall be cleaned and rescanned promptly upon discovery of malicious code.

5.1.12. Incidents involving malicious code shall be resolved in accordance with DAS Procedure: Incident Response. Resolutions should include consideration of any need to preserve legal evidence.

Reporting

5.1.13. DAS Programs shall establish a point of contact (POC) that will either provide support directly, or can serve as an intermediary to get support for affected systems.

5.1.14. DAS Programs shall establish procedures for reporting malicious code incidents internally to their designated Program POC and shall adhere to DAS Procedure: Incident Response regarding other incident response reporting requirements.

5.1.15. DAS Programs shall document malicious code incidents for auditing purposes and provide summary reports to the Office of Information Security and Privacy in accordance with DAS Procedure: Incident Response.

5.1.16. All the steps taken to recover from a malicious code incident shall be documented. These steps shall be used for future reference in updating procedures and educating personnel.

5.1.17. When feasible, employees shall inform the system administrator or Program POC immediately of any different or out of the ordinary behavior that a device or application exhibits or any malicious code detected. Suspected or confirmed

malicious code incidents shall be reported in accordance with DAS Procedure: Incident Response.

5.1.18. When informed that a virus or other malicious code has been detected and is likely to be widespread, the system administrator or POC shall inform all users who may have been exposed to the same programs or data that malicious code may have infected their systems. Additional required actions may be specified in DAS Procedure: Incident Response.

5.1.19. After the confirmation of the existence of a widespread malicious code infiltration, the system administrator shall notify a predetermined list of potentially infected users of the steps necessary to determine if their system is infected and the steps to take to remove the malicious code. Additional required notifications may be specified in DAS Procedure: Incident Response.

5.1.20. DAS Programs shall report to the Office of information Security and Privacy the quantity and location of systems that bypass malicious code scanning. A written variance must be obtained and maintained for all systems deviating from this policy via DAS' Policy Exemption/Deferment Request process.

5.2 Individual Responsibilities

Specific responsibilities regarding use of IT resources are detailed in DAS Policy 700-01: IT Resource Usage and DAS Policy 2100-02: Mobile Computing. In addition, each employee, contractor, temporary worker or other agent of the state who operates a privately-owned desktop, laptop, or other computing device authorized for use with systems or networks owned or operated by DAS is responsible for:

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 or changing anti-virus or other anti-malware software.
5.2.4. Reporting any malicious code encountered or other similar activity in accordance with DAS Procedure: Incident Response.
5.2.5. Properly installing and using up-to-date anti-virus and/or other anti-malware software consistent with Ohio IT policy and DAS policy and practice with regard to privately-owned computers authorized for use for DAS business.

5.3 Malicious Code Awareness Training

5.3.1. DAS shall include appropriate malicious code security education and awareness efforts as part of DAS' overarching security education and awareness program. As a minimum, these efforts shall include providing information concerning the risks malicious code presents to restricted and other sensitive data.

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

5.4 Procurement

5.4.1. DAS 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.
- Any non-state computing or telecommunications devices used to fulfill state contracts are free from known malicious code.

6.0 RELATED PROCEDURES

DAS Procedure: Incident Response
DAS Procedure: Install New Servers
DAS Procedure: Monitoring Server Policy Compliance
DAS Procedure: Server Anti-Virus Administration Updates
DAS Procedure: Vulnerability Scanning
DAS Procedure: Windows Patch Management
DAS Procedure: Workstation and Desktop Configuration

Additional standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy.

At a minimum:

- This policy shall be distributed to each newly hired DAS employee during orientation, in conjunction with other applicable policies, procedures, and standards; the new employee shall sign an acknowledgement of receipt of this policy.
- Vendors, contractors, and temporary employees shall receive a copy of and sign an acknowledgement of receipt of this policy prior to gaining access to IT resources.

7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

8.0 DEFINITIONS

DAS – Department of Administrative Services.

DAS Contractors – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

DAS Employees – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

DAS–owned – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

DAS–provided or **DAS-supplied** – Made available to users by DAS.

IT Resources – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

Malicious Code – Collective term for program code or data that is intentionally included in or inserted into an information system, application, or device for unauthorized purposes. Examples include viruses, logic bombs, Trojan horses, worms, key loggers, and spyware. Often used interchangeably with the term **Malware.**

Malware – See **Malicious Code**.

Management – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

OIT – Office of Information Technology.

Privately–owned - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

State–owned - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

System Assets – System assets include information, hardware, software, and services required to support the business of DAS and identified during the risk assessment process as assets that require protection.

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 IT Resources on behalf of the state.

9.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, Suite 4083
Columbus, Ohio 43215
Telephone: 614.644.9391
Email: state.isp@oit.ohio.gov
Web: infosec.ohio.gov

Department of Administrative Services policies can be found online at:

http://das.ohio.gov/Divisions/DirectorsOffice/EmployeesServices/DASPolicies/tabid/463/Default.aspx

10.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 12/07/07
12/05/2012	Policy reissued under Director Robert Blair.

11.0 ATTACHMENTS

None.