Ohio Supercomputer Center Intrusion Prevention and Detection	**No:** **OSC-12**
	Effective: **5/21/09**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

The purpose of this state policy is to establish an ***intrusion*** prevention and detection capability that is designed to prevent, monitor and identify system intrusions or misuse.

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

Threats that penetrate an organization's boundary can come from a variety of sources, such as visitors with insecure laptops, inappropriate use of the ***Internet***, or insiders attempting to gain unauthorized privileges. To help counter these threats, tools, methods and processes have evolved that identify, document and defuse such attacks or intrusions.

Intrusion detection is the process of detecting unauthorized usage, anomalies or attacks on computer, network or telecommunications systems. ***Intrusion detection systems*** help protect information ***system assets*** by identifying or assessing system weaknesses and alerting the organization when a possible intrusion has occurred.

Intrusion prevention extends the functionality of intrusion detection by anticipating, monitoring and stopping events that may stem from possible misuse. ***Intrusion prevention systems*** represent a natural progression in security technology and offer the opportunity to build upon previously implemented technologies to create a multi-layered security solution that will further protect system assets. However, intrusion prevention systems must be carefully configured and employed to ensure that the systems do not interfere with valid activities.

Both intrusion prevention and intrusion detection systems are designed to prevent attempts to compromise the ***confidentiality***, ***integrity*** or ***availability*** of an information technology asset. Agencies may choose to adopt these systems in their efforts to cultivate an overall intrusion prevention and detection capacity, which may include other security controls, such as security assessments, ***vulnerability scanning***, patch management and security audits.

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 information technology 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 security policy for state information and services. Ohio IT Policy ITP-B.12, "Intrusion Prevention and Detection," is one of several subpolicies. 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 Ohio IT Bulletin ITB-2006.01, "Public Records Requests Concerning IT and Telecommunications Systems," effective August 29, 2006, notifies state agencies that Ohio's public records law exempts certain types of security and infrastructure records from mandatory release to protect critical information regarding agency security practices and vulnerabilities. Agencies are advised to review closely all IT-related public records requests with legal counsel and to ensure that security records and infrastructure records have been properly identified as required in Ohio IT Policy ITP-B.1, "Information Security Framework," and section 149.433 of the Ohio Revised Code.

4.6 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

OSC establishes this intrusion prevention and detection policy in compliance with the state policy and ensures adherence to said policy. OSC will deploy intrusion prevention and detection capabilities as part of an overall, multi-layered information technology

security design to prevent, monitor and identify system intrusions or misuse. The policy includes the following elements:

5.1 Assessment. OSC shall develop and deploy intrusion prevention and detection guidelines, systems and procedures for assets identified as critical to the mission of the agency. Such assessments can be enhanced or developed using vulnerability tools such as ***discovery scanning*** or vulnerability scanning.

5.2 Implementation of Intrusion Prevention and Detection Capabilities. OSC shall evaluate, select and deploy intrusion prevention and detection capabilities compatible with the network infrastructure, policies and resources. OSC intrusion prevention and detection capabilities shall address the following:

5.2.1 Personnel. Personnel shall be identified and properly trained to operate, interpret and maintain intrusion prevention and detection capabilities. A ***vetting process*** commensurate with the risk associated with an asset shall be applied to job applicants for positions in which they are to be charged with protecting an information asset.

5.2.2 Assets. Intrusion prevention capabilities shall be implemented to prevent unauthorized use, anomalies or attacks on computer, network or telecommunications systems. In addition, intrusion detection capabilities shall be in place to provide information related to unauthorized or irregular behavior on an agency computer, network or telecommunications system.

Intrusion prevention and detection capabilities shall be implemented that encompass basic security procedures such as reviewing activity logs, and depending on the results of the assessment, may also include special-purpose intrusion prevention and detection features such as those found on ***network-based***, ***host-based, wireless***, ***or network behavior analysis intrusion prevention and detection systems***.

5.2.3 Prevention Controls. OSC will employ intrusion prevention systems that take action in response to a perceived attack shall carefully review the planned actions from the perspective of continuing service to meet business objectives, and shall ensure that the risk assessment and trade-off is considered.

5.3 Monitoring, Review & Detection. intrusion prevention and detection capabilities shall include guidelines for monitoring and analyzing ***system logs***, notifications, warnings, alerts and ***audit logs*** in accordance with Ohio IT Policy ITP-B.1, “Information Security Framework.” Agencies shall maintain and review information technology security audit logs and intrusion prevention and detection system alerts on a regular basis to determine if an intrusion or other type of security ***incident*** has occurred.

5.3.1 Security Audit Strategies. OSC shall develop information technology security audit strategies and processes relevant to each system. The

strategy shall include the definition of monitored assets, the types and techniques of intrusion prevention systems or intrusion detection systems to be used, where each intrusion prevention system or intrusion detection system will be deployed, resources responsible for monitoring, the types of attacks the intrusion prevention systems or intrusion detection systems will be configured to prevent or detect, and the methods that will be used for responses or alerts.

5.3.2 Alarms and Alerts. Thresholds for alarms and alerts shall be configured to identify possible intrusion prevention or detection events or violations of agency policy. Agency procedures shall address the disposition, retention and criticality of alerts.

5.4 Incident Response. OSC will respond to security incidents in compliance with OSC Policy, OSC-7, OSC Security Incident Response.

5.5 Education and Awareness. OSC shall provide education to all personnel engaged in the intrusion prevention and detection. Awareness education shall incorporate incident awareness and reporting guidelines.

5.6 Public Records Requests. Elements of this policy involve the creation of records that may be considered security records not subject to disclosure under Ohio's public records law. When considering public records requests that are related to security or infrastructure records, refer to Ohio IT Bulletin ITB-2006.01, "Public Records Requests Concerning IT and Telecommunications Systems," for additional guidance on disclosure requirements.

6.0 Procedures

None.

7.0 Implementation

This policy is effective immediately.

8.0 Revision History

Date	Description of Change
6/1/2009	Original policy.

9.0 Definitions

9.1 Audit Logs. A record showing who has accessed a computer system and what operations have been performed during a given time period. Audit logs are useful both for maintaining information technology security and recovering lost transactions.

9.2 Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.

9.3 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

9.4 Discovery Scanning. A network evaluation that examines an agency's network configuration and deployed system resources. Identified resources are compared to an authoritative list of known and approved agency resources and services so that unauthorized resources or configurations can be investigated.

9.5 Host-based Intrusion Prevention and Detection System. A program that monitors a single host to identify and stop suspicious activity. A host-based intrusion prevention system has the ability to apply policies based on pre-defined rules or learned behavior analysis to a particular computing device to block malicious server or personal computer actions. A host-based intrusion prevention system has the ability to stop attackers from implementing buffer overflow strikes, changing registry keys, overwriting dynamic link libraries or engaging in other approaches to obtain control of the operating system. A host-based intrusion detection system analyzes the activity on a particular computing device and monitors for attack signatures and system anomalies such as system processes, registry entries, central processing unit and memory usage, file access and integrity checking.

9.6 Incident. A reported security event or group of events that has proven to be a verified information technology security breach. An incident may also be an identified violation or imminent threat of violation of information technology security policies[2], or a threat to the security of system assets. Some examples of possible information technology security incidents are:

- Loss of confidentiality of information
- Compromise of integrity of information
- Loss of system availability
- Denial of service
- Misuse of service systems or information
- Damage to systems from malicious code attacks, such as viruses, Trojan horses or logic bombs

9.7 Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of data in state databases, agencies must ensure that data is protected from improper change. Information systems

that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.

9.8 Internet. A worldwide system of computer networks — a network of networks — in which computer users can get information and access services from other computers. The Internet is generally considered to be public, untrusted and outside the boundary of the state of Ohio enterprise network.

9.9 Intrusion. An unauthorized entry into a network or system. Frequently synonymous with an information technology security incident.

9.10 Intrusion Detection System. An information technology security system that monitors computer systems and network traffic and analyzes that traffic for potential hostile attacks originating from both within and external to an organization or agency.

9.11 Intrusion Prevention System. An information technology security system that monitors computer systems and network traffic, analyzes that traffic for potential hostile attacks originating from both within and external to an organization or agency, and blocks or prevents the hostile attack from causing damage.

9.12 Network-Based Intrusion Prevention and Detection System. A network-based intrusion prevention system resides inline on the network to intercept and inspect all inbound or outbound network packets. The intrusion prevention system performs a range of detection analyses, not only on each individual packet, but also on network conversations and patterns, viewing each transaction in the context of others. Based on these observations, the intrusion prevention system will either block traffic or pass it along through the network. A network-based intrusion detection system detects attacks or system misuse by capturing and analyzing network packets or traffic flow using techniques such as ***traffic analysis***, protocol anomaly detection, signature based detection, and statistical/behavioral analysis. Information can be compared to a database of known attack signatures, anticipated misuse or anomaly profiles.

9.13 Network Behavior Analysis System. An intrusion prevention and detection system that examines network traffic to identify and stop threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware, and policy violations.

9.14 Rogue Wireless Device. An unauthorized wireless station (client) or access point operating within the boundary of the agency's facilities.

9.15 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."

9.16 System Logs. A file that lists the actions that have occurred. System logs facilitate analysis tools to assist in determining where users are coming from, how often, and their navigation path.

9.17 Traffic Analysis. An analytical technique that maps the flow of an activity, focusing on the source, path and destination of the activity. Traffic analysis may provide an analyst with the ability to infer the purpose or data content associated with the activity.

9.18 Vetting Process. A verification process used to validate the identity and trustworthiness of a person who is seeking access to computer systems and networks.

9.19 Vulnerability Scanning. A scan that examines both network and system configuration security preparedness. Identified network and host system weaknesses are compared to known security weaknesses, including the absence of security-related patches.

9.20 Wireless Intrusion Prevention and Detection System. An intrusion prevention and detection system that monitors wireless network traffic and analyzes wireless networking protocols to identify and stop suspicious activity originating from unauthorized devices such as laptops, cell phones, personal digital assistants or other ***rogue wireless devices***.

10.0 Related Resources

Document Name
Ohio IT Bulletin ITB-2006.01, "Public Records Request Concerning IT and Telecommunications Systems," regarding public records requests related to security and infrastructure records may be found at: www.ohio.gov/itp.
National Institute of Standards and Technology's "Guide to Intrusion Detection and Prevention Systems (IDPS)." http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

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