Ohio Supercomputer Center Security Education and Awareness	**No:** **OSC-6**
	Effective: **06/02/2009**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

This policy requires OSC to provide information technology security education and awareness to employees, contractors, temporary personnel and other agents of OSC who use and administer computer and telecommunications systems.

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

Effective information technology security includes security awareness and individual responsibility. OSC personnel should understand why and how information technology security is implemented. Without understanding and buy-in, OSC personnel are likely to view security measures as a hindrance. Since personnel play a critical role in an OSC's security profile, inadequate education and awareness can lessen an agency's ability to adequately safeguard its information technology assets and information. According to the System Administration, Networking, and Security Institute, "Every employee should have security awareness training, because every employee must act in a secure manner for the whole organization to be reasonably safe from 'people-oriented' vulnerabilities."[1] For an agency's information technology security to be most effective, personnel should be routinely informed of security measures that have been deployed so that they understand why the measures exist and how they align with the agency's business objectives.

[1] Hubbard, William. "Methods and Techniques of Implementing a Security Awareness Program." GSEC Practical Assignment, version 1.3. 8 April 2002. <www.sans.org/rr/papers/47/417.pdf>.

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 OSC IT Policy, OSC-3, "Information Security Framework," is the overarching security policy for OSC information and services. OSC IT Policy OSC-6, "Security Education and Awareness," 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.11, "Data Classification," provides a high-level data classification methodology to state agencies for the purpose of understanding and managing data and information assets with regard to their level of confidentiality and criticality.

4.4 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.

4.5 Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data," effective July 25, 2007, outlines the requirements for the encryption of sensitive data as well as requirements for securing portable devices and media, backups, sensitive data in transmission, and sensitive data at rest. The bulletin also outlines restrictions for sensitive data, physical security considerations, public servant acknowledgement requirements, and incident response.

4.6 A glossary of terms for 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 an information technology education and awareness policy in compliance with state policy and shall ensure that all employees, contractors, temporary personnel and other agents of OSC adhere to that policy. An OSC designee shall be

assigned to administer the policy and ensure compliance. The policy shall address the elements specified in sections 5.1 through 5.7 below.

5.1 Security Awareness. OSC shall conduct ongoing information technology security awareness programs for all personnel. At a minimum, awareness efforts shall include:

5.1.1 How the OSC information technology security policies meet the business objectives of the agency, identifying the information, hardware, software and services required to support the business of the agency and that need to be protected.

5.1.2 Identification of the most likely threats to the information technology environment, such as:

Insider abuse and mistakes
Viruses and other ***malicious code***
Unauthorized access
Deception for the purpose of obtaining confidential information or information that could compromise security
Inadequate password creation, protection and maintenance
Data theft

5.1.3 An overview of the ***risk management*** process the agency uses to comply with the risk assessment requirements in OSC IT Policy OSC-3, "Information Security Framework."

5.1.4 Identification of security responsibilities for all personnel levels, including, but not limited to:

Compliance with all password requirements
Physical security
Workstation security
Portable computing security
Reporting security events
Data retention, safeguarding and ***disposal***

5.1.5 Identification of reporting requirements to the agency information technology security point of contact as defined in OSC IT Policy OSC-3, "Information Security Framework."

5.2 General Information Technology Security Education. OSC will incorporate information technology security education as part of the orientation for new employees, contractors, temporary personnel and other agents of the university. Thereafter, education programs shall be offered at least biennially. At a minimum, such education shall include:

5.2.1 A description of the elements of the risk management process as defined in OSC IT Policy OSC-3, , "Information Security Framework," and its application to the OSC's environment.

5.2.2 A description of OSC information technology security policies, how they mitigate risk, and how they complement the business objectives of the state.

5.2.3 A description of data classification as defined in OSU Policies on Data Classification, and its application to the OSC environment.

5.2.4 A description on the Ohio State University policy on Institutional Data.

5.2.5 A review of the applicable laws, regulations and state policies, including state and individual liabilities.

5.2.6 Consequences of noncompliance with university and state information technology security policies, related laws, regulations and other policies.

5.2.7 A summary of OSC security ***incident response*** procedures, including identification of the reporting hierarchy and the OSC security ***incident*** point of contact.

5.3 Technical Education. Technical information technology security education shall be administered on a frequency that is consistent with changes in technology for individuals responsible for implementing secure solutions. OSC shall determine the appropriate types of technical education for employees and other agents of the university.

5.3.1 Technical education may include, but not be limited to, training, certification, formal coursework, and conferences for information technology security technologies and practices, such as:

Firewalls
Wireless
Routers
Switches
Virtual private networks
Encryption
Public key infrastructure
Security procedures and methodologies
Implementing secure solutions at each stage of the ***software development lifecycle***
Preventing, reporting and responding to information technology security incidents
Risk assessment
Data protection
Audit logging

5.4 Executive Education. Designated personnel at OSC shall report at least annually, to executive-level personnel, including chief information security officers or the equivalent, on the state of OSC's information technology security profile. At a minimum, such reporting shall include the following elements, specific to the agency:

5.4.1 OSC and individual roles, responsibilities and liabilities.

5.4.2 Current risk assessment, security management and incident response capabilities of the OSC.

5.4.3 Current threats.

5.4.4 Current countermeasures.

5.4.5 Deficiencies of applicable resources.

5.4.6 Status of security incidents.

5.4.7 Impact of security incidents.

5.4.8 Incident response successes and failures.

5.4.9 Division of responsibilities during an information technology security incident.

5.4.10 Internal and public ***communication schedules*** for an information technology security incident.

5.4.11 A description of OSC information technology security policies and the rationale of how they mitigate risk and complement the business objectives of the state.

5.5 Measures and Records. Records of information technology security education efforts shall be maintained. Metrics which help to illustrate the effectiveness of education efforts shall be maintained by OSC and referenced during subsequent education development. Security education and awareness efforts shall be reviewed and updated periodically to reflect new trends, threats and OSC information technology security breaches.

5.6 Methods. OSC shall determine the appropriate methods used for awareness and education, which may include but are not limited to:

Posters
Computer-based training
Intranet materials and resources
Videos
Newsletters
Memoranda

Briefings
Formal classroom instruction
On-the-job training
Conferences

5.7 Public Records Requests. Elements of this policy involve the creation of records that may not be 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. Such requests will be referred to the OSU Office of Legal Affairs.

6.0 Procedures

None.

7.0 Implementation

This policy is effective immediately.

8.0 Revision History

Date	Description of Change
6/2/2009	Original policy.

9.0 Definitions

9.1 Communication Schedules. A pre-defined structure that delineates the communication strategy for a given event. Elements include who delivers communications, which personnel are the intended recipients, the format of the communications, and the timeline and a record of the accomplishment of each. Communication schedules are implemented in business continuity and risk management planning or other situations where senior officials must ensure that information is disseminated.

9.2 Disposal. The final transfer of ownership or custody of an information technology device.

9.3 Encryption. The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

9.4 Firewall. Either software or a combination of hardware and software, that implements security policy governing traffic between two or more networks or network segments. Firewalls are used to protect internal networks, servers and

workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a notebook computer, and must be configured properly to enable protection.

9.5 Incident. A reported adverse event or group of adverse 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

9.6 Incident Response. A structured and organized response to any information technology security adverse event or incident that threatens an agency's system assets, including systems, networks and telecommunications systems.

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 Intranet. A private network contained within an enterprise whose purpose is to aid employees in sharing information and computing resources. It may consist of many linked local area networks and may also include leased lines in a wide area network. An intranet may include connections through one or more gateway computers to the outside Internet. Intranets are commonly used to facilitate working in groups and to hold teleconferences.

9.9 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.

9.10 Packet Filtering. A process that allows or denies an Internet Protocol (IP) packet based upon criteria in the packet header. Filtering decisions can be based upon the source address of the packet, the destination address, the protocol and the port. Packet filtering is typically implemented on routers or general-purpose

[2] Grance, Tim, Karen Kent, and Brian Kim. Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. January 2004. < http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>.

computers acting as routers for a network or network segment. Packet filtering is generally effective to control services like Simple Mail Transfer Protocol (SMTP, used for e-mail transmission), Hypertext Transfer Protocol (HTTP, used for Web page transmission) or Network Time Protocol (NTP, used to synchronize time). For services such as Domain Name Service (DNS, which translates names into IP addresses) and File Transfer Protocol (FTP, used to upload files to and download files from the Internet), the more complex security controls available only in proxies may be required.

9.11 Public Key Infrastructure. The technical, procedural and management infrastructure to use public key cryptography. Public key cryptography uses a public and private key pair to provide services such as encryption, non-repudiation and digital signatures. Both keys are needed for public key cryptography to work. A public key infrastructure (PKI) manages the distribution of public and private keys and provides a level of assurance for users by maintaining lists of which keys are valid.

9.12 Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security. See Ohio IT Policy ITP-B.1, "Information Security Framework," for assessment guidelines.

9.13 Risk Management. A discipline that includes the processes concerned with identifying, analyzing and responding to information technology security risks. Risk management attempts to maximize the results of positive events and minimize the results of negative events.

9.14 Router. A network traffic control device that implements network policy and provides a measure of control for traffic entering and leaving a network. Routers help ensure that network traffic reaches its intended destination. During the routing process, routers can implement ***packet filtering*** based on network traffic packet content and discard packets that do not adhere to network policy.

9.15 Software Development Lifecycle. The software development lifecycle is a framework for developing information systems and software. The software development lifecycle is built on eight phases: concept, requirements, design, development, testing, documentation and training, deployment, and post-deployment. Each phase in the software development lifecycle has associated activities, deliverables, and exit criteria.[3]

9.16 Switch. A network device that selects a path or circuit for sending data to its next destination. Some switches have evolved to include the functions of a router.

[3] Ohio Office of Information Technology. Investment and Governance Division. Enterprise Project Management Office. Project Management Community of Practice. < http://pmcop.ohio.gov/>.

9.17 Virtual Private Network. A private network that is configured within a public network. Virtual Private Networks operate as private national or international networks to the customer, while physically sharing backbone links with other customers. Virtual Private Networks provide security similar to a private network using access control and encryption, but take advantage of the economies of scale and built-in management facilities of public networks.

9.18 Wireless. Use of various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on a hardwired connection, such as twisted pair, coaxial or fiber optic cable.

10.0 Related Resources

Document Name
Federal Information Security Management Act of 2002 (Public Law 107-347, Dec. 17, 2002, 116 STAT. 2946)
Ohio IT Bulletin ITB-2006.01, "Public Records Requests Concerning IT and Telecommunications Systems," regarding public records requests related to security and infrastructure records may be found at: www.ohio.gov/itp.
Ohio IT supplemental educational materials supporting each security policy including technical white papers, implementation tips, audit checklists and user responsibilities may be found at: www.ohio.gov/itp.
The Ohio State University policies and supplemental information may be found at: www.osu.edu/policies.

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