Ohio Supercomputer Center Security Notifications	**No:** **OSC-10**
	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 OSC policy identifies the methods used to inform users of their duty, limitations on use, legal requirements and personal privacy expectations associated with the use of OSC and university computers, networks or 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

Applications and network systems are experiencing increased incidents of intrusion, attacks and misuse. According to the National Institute of Standards and Technology, "Security related threats have become not only more numerous and diverse but also more damaging and disruptive."[1] ***Security notifications*** provide the opportunity to disclose the potential legal implications of unauthorized access, information misuse, and data loss and corruption. Notifications are also used to define agency guidelines and expectations for system access and usage.

[1] Grance, Tim, Karen Kent, and Brian Kim. "Computer Security Incident Handling Guide." National Institute of Standards and Technology. January 2004. <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.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 state information and services. OSC IT Policy OSC-10, "Security Notifications," is one of several subpolicies. These security policies should be considered collectively rather than as separate or unrelated policies.

4.3 OSC IT Policy OSC-6, "Security Education and Awareness," requires OSC to provide information technology security education and awareness to employees and other agents of the university.

4.4 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 as an agency of the State of Ohio is required to establish a security notification policy that is in compliance with state policy and ensure that all users adhere to that policy. OSC shall use security notifications for all ***public systems*** and ***nonpublic systems***, including Web-based applications.

5.1 Security Notification Content. Security notifications shall include the following elements:

- The system is designated for official university use.
- Access to the system may be logged.
- System activity may be monitored and logged.
- Users shall comply with OSC information technology policies.
- Users shall have no expectation of personal privacy unless explicitly stated.
- Illegal or unauthorized attempts to access the system and information could lead to criminal penalties and civil liability.

5.2 Security Notification Methods. OSC will present security notifications using ***active***, ***informational*** or ***passive*** notification methods in an apparent and obvious manner. The notification method shall be determined by the agency based on the risk assessment of the ***system assets*** as defined in OSC IT Policy OSC-3, "Information Security Framework."

5.3 Compliance Review. OSC shall conduct a compliance review of all security notifications with relevant staff (ie. IT, policy, communications, and legal personnel) prior to their deployment. The compliance review shall determine if the security notification:

- Complies with overall OSC, University and state policies; and
- Conforms to federal, state or local laws.

5.4 Education and Awareness. Agencies shall establish security notification education and awareness efforts in accordance with Ohio IT Policy ITP-B.8, "Security Education and Awareness." Awareness education should provide an overview of why security notifications are necessary, the types of notifications, and the justification behind employing each of the various types.

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 Active Security Notifications. A type of security notification that is presented in an apparent and obvious manner during system ***identification and authentication*** procedures. Active security notifications are presented before access is granted to the system or data and include an acknowledgment of the notification. An example of an active notification method is a "click through" box.

9.2 Identification and Authentication. The verification of the identity of a requesting entity (a person, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques, such as user ID, password, personal identification number, digital certificates, ***security tokens*** or biometrics, to enforce I&A, depending upon the level of access control required to protect a particular system.

9.3 Informational Security Notifications. A type of security notification that is presented in an apparent and obvious manner during system identification and authentication procedures. Informational security notifications are presented

before access is granted to the system or data. This type of notification does not require a user acknowledgement.

9.4 Nonpublic System. A state computer or telecommunications system for use only by employees, contractors, temporary personnel and other agents of the state. Examples of such systems include payroll or benefit related systems that do not grant the general public access.

9.5 Passive Security Notifications. A type of security notification that does not require the presentation of security notification information as part of system identification and authentication procedures. Examples of passive security notifications are as follows:

- Security notifications presented outside the system identification and authentication procedures
- Security notification Web links
- User authorization agreements
- System or terminal stickers
- Orientation agreements for employees, contractors, temporary personnel and other agents of the state

9.6 Public System. A state computer or telecommunications system used in whole or in part by individuals such that the use is not based on employment or contractual relationships with the state. Examples of such systems would include online applications provided by agencies that allow users from the general public to execute transactions, request documentation, or view personal information.

9.7 Security Notifications. An apparent or obvious statement that describes a limitation on use, a duty, or a restriction, and possible consequences for illegal or unauthorized access or attempted access to a system.

9.8 Security Token. A portable, physical device that enables pre-approved access to data or systems. An example is a security-enabled key fob.

9.9 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.”

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