Ohio Supercomputer Center Remote Access Security	**No:** **OSC-5**
	Effective: **5/21/2009**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1.0 Purpose

This policy is to establish practices wherever a ***remote access*** capability is provided to OSC systems so that inherent vulnerabilities in such services may be compensated.

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

Remote computer access is a popular method of accomplishing work away from the office while at home or while traveling. However, remote access capabilities can add security vulnerabilities because such services increase the number of access points that hackers can use to gain entry. It is critical that these access points be properly secured.

This policy establishes the security requirements for OSC having responsibility for ownership, operation or maintenance of an information system environment that provides remote access. Because many state agencies now permit the business use of computers that are not owned by the state or universities, the network perimeter has been extended to include those computers. However, it should not be implied that this policy requires agencies to be responsible for the installation, maintenance and support of computers and personal digital assistants that are not owned by the state.

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.5, "Remote Access 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.2, "Boundary Security," requires that state agencies implement and operate a robust network perimeter defense capability. Users of state electronic services must be provided with secure and reliable access to resources and communication. Unauthorized users must be detected and denied access.

4.4 Ohio IT Policy ITP-B.3, "Password and Personal Identification Number Security," establishes minimum requirements regarding the proper selection, use and management of passwords and personal identification numbers.

4.5 Ohio IT Policy ITP-B.6, "Internet Security," requires agencies to implement and operate security protections for Internet, extranet and intranet use, and Internet security awareness training of employees, contractors, temporary personnel and other agents of the state.

4.6 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.

4.7 Ohio IT Standard ITS-NET-01, "802.11 Wireless Local Area Network," defines minimal requirements for the configuration and use of existing or newly implemented IEEE 802.11 wireless local area networks within state government.

4.8 Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," defines minimal requirements for the encryption of sensitive data within state government.

4.9 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

5.1 Authentication. OSC shall authenticate all remote users. Only pre-approved users shall have access to OSC systems. At a minimum, a user ID and password is required.

For data and other ***system assets*** identified in the risk assessment as requiring secure access, use ***two-factor authentication*** to limit access to systems that contain data requiring more secure access or information whose disclosure would cause serious disruption or harm.

5.2 Data Access. OSC shall limit remote access to university data based on The Ohio State University defined data classification guidelines and limitations for downloading data in accordance with OSU IT Policy "Policy on Institutional Data."

5.3 Privileges. OSC shall establish and implement a procedure for how a user is granted permission for remote access privileges following the ***least-privilege*** method. The procedure shall also address methods for revoking the remote access privileges of users who no longer need such access.

5.4 Remote Connections. Users shall not establish a separate Internet connection while simultaneously connected to an agency network through the use of multiple network cards, modems or other access techniques.

5.5 Dial-In. At a minimum, limit the quantity of dial-in numbers to that which is needed; limit the number of persons who are privy to the dial-in numbers; and require a valid, active user account. Whenever possible, prevent display of remote access dial-in numbers.

5.6 Records. OSC shall establish and implement a procedure for keeping their directories of approved users and dial-in numbers accurate, current and protected.

5.7 Internet. OSC secures the internet connection in accordance with Ohio IT policies ITP-B.2, "Boundary Security," and ITP-B.6, "Internet Security."

5.8 Host Security. OSC shall ensure that all remote access ***host*** servers are securely configured. As a minimum:

5.8.1 Ensure that a system's security configuration is appropriate to support OSC mission and functions.

5.8.2 Regularly examine audit logs and comply with the security audit logging requirements addressed in OSC IT Policy OSC-12, "Intrusion Vulnerability and Detection."

5.8.3 Turn off all system operating facilities that are not required.

5.8.4 Authorize remote access to each server only to those users with a demonstrated need.

5.8.5 Test vendor vulnerability ***patches*** to verify that they do not introduce problems into OSC systems. Apply verified patches as soon as possible.

5.8.6 Develop migration plans for operating systems that are scheduled to be discontinued or unsupported by the vendor.

5.10.7 Ensure that all host servers are protected in accordance with Ohio IT Policy ITP-B.2 "Boundary Security."

5.11 Encryption. At a minimum, passwords that are transmitted shall be encrypted. Data requiring secured access as determined by the risk assessment according to the risk management section of Ohio ITP Policy ITP-B.1, "Information Security Framework," shall be encrypted for transit between remotely accessed systems in accordance with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography."

6.0 Procedures

None.

7.0 Implementation

The policy is effective immediately upon adoption

8.0 Revision History

Date	Description of Change
6/1/2009	Original policy.
03/19/2012	Scheduled policy review.

9.0 Definitions

9.1 Biometrics. Biological characteristics such as fingerprint, face or retinal blood vessel patterns used by authentication devices to allow an individual access to information, services or other resources.

9.2 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.

9.3 Host. A platform that runs an application.

9.4 Least-Privilege. A method for assigning privileges in a system. The objective is to assign only those privileges that are necessary to perform the required functions, and ensure that other privileges are not assigned and cannot be improperly accessed. For example, a typical system user should not be assigned rights to read, write and execute all of a department's files when the user only requires the ability to read a subset of these files to do an assigned job.

9.5 Patch. A procedure or software that corrects a malfunction or security vulnerability of a system.

9.6 Remote Access. An activity or service that enables a user to connect to a network when the user is at a physical location apart from that of the network.

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

9.8 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."

9.9 Two-factor Authentication. Authentication that incorporates two elements. There are three elements of authentication: "what you know" (for example, a password or PIN), "what you have" (for example, a digital certificate, ***security token*** or a smart card), and "what you are" (for example, a ***biometric***). Two-factor authentication is commonly used for access to systems that contain data requiring secured access or information of which disclosure would cause serious disruption or harm. It is also known as strong authentication, although strong authentication can have more than two elements.

9.10 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
Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," available at www.ohio.gov/itp.

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