Ohio Supercomputer Center Portable Security Computing	**No:** **OSC-09**
	Effective: **05/27/09**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** TBD

1. **Purpose**

   This policy addresses information technology (IT) security concerns with ***portable computing devices*** and provides direction for their use, management and control. This policy includes security concerns with the physical device itself, as well as its applications and ***data***.

2. **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. **Background**

   A deliberate decision needs to be made on whether or not portable computing devices should be allowed and, if so, to what degree the devices would be supported. It is essential to address the use and maintenance of state-owned and privately-owned portable devices, protection of sensitive data, adherence to legal requirements, and the safeguarding of ***system assets***.

   Portable computing devices are increasingly becoming an integral tool for government agencies and businesses. Through the use of portable computing devices, ***users*** are able to access university computer and telecommunications systems so that they can work remotely outside of traditional business hours and while traveling.

   One consequence of this ability has been the co-mingling of business and personal computing assets, particularly portable computing devices such as notebook computers and personal digital assistants. Government agencies need to ensure that the appropriate

safeguards are in place to protect against the intentional or inadvertent corruption or destruction of system assets.

4. References

This Policy is based on the following State of Ohio Policies:

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 security policy for state information and services. Ohio IT Policy ITP-B.9, "Portable Computing Security," 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.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 communications. 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.4, "Malicious Code," requires state agencies to implement and operate a malicious code security program. The program should help to ensure that adequate protective measures are in place against introduction of malicious code into state-controlled information systems and that computer system users are able to maintain a high degree of malicious code awareness.

4.6. Ohio IT Policy ITP-B.5, "Remote Access," requires state agencies to implement and operate security measures wherever a remote access capability is provided to state systems so that inherent vulnerabilities in such services may be compensated.

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

4.8. 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.

4.9. Ohio IT Policy ITP-E.1, "Disposal, Servicing and Transfer of IT Equipment," establishes agency requirements for the disposal, servicing or transfer of state agency IT equipment with regard to state data, licensed software and intellectual property, and rechargeable batteries and other hazardous materials.

4.10. 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.

5. Policy

This policy is not intended to address the use of portable devices by the general population to access electronic OSC services.

In addition to state-owned portable computing devices, the policy shall address privately-owned and contractor-owned portable computing devices authorized for university use by the agency or as an agent of the university. OSC policy shall address the following:

5.1. Physical Security. OSC and users shall protect university-owned and university-authorized portable computing devices, removable storage components and removable ***computer media*** from unauthorized access. Physical security measures shall incorporate at a minimum the practices listed below in 5.1.1 through 5.1.4.

5.1.1. Portable computing devices, computer media and removable components, such as ***disk drives*** and network cards, shall be stored in a secure environment. Devices shall not be left unattended without employing adequate safeguards, such as cable locks, restricted access environments or lockable cabinets.

5.1.2. When possible, portable computing devices, computer media and removable components shall remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device, computer media and removable components.

5.1.3. Safeguards shall be taken in public or common areas to avoid unauthorized viewing of sensitive or confidential data.

5.1.4. OSC will maintain an inventory for all university, privately-owned and contractor-owned portable devices authorized for work use with university systems. The inventory shall include the device make, model, serial number, date introduced into service and party responsible for the device.

5.2. Operation and Maintenance. OSC shall establishes and implements IT security procedures for the secure operation and maintenance of portable computing devices.

5.2.1. Anti-virus software. Portable computing devices shall be equipped with anti-virus software in accordance with OSC Policy OSC-4, "Malicious Code Security."

5.2.2. System configuration. Mandatory system configurations, settings and software for either university-owned or authorized non-university owned devices shall not be modified without prior authorization by designated OSC personnel. Device operating systems shall be maintained with appropriate vendor security patches and updates.

5.2.3. Portable computing devices shall not be equipped with remote system or application ***administrator privileges*** unless authorized. Portable computing devices equipped with remote system administrator capabilities shall be assigned higher levels of security in accordance with the increased risk of an IT security breach or loss of the device, pursuant to OSC Policy OSC-3, "Information Security Framework."

5.2.4. OSC or university data, applications and other system resources stored on portable computing devices shall be secured in accordance with the OSC risk assessment as defined in OSC Policy OSC-3, "Information Security Framework." Methods for securing information maintained on portable devices may include as applicable, but not be limited to:

- Personal ***firewalls***
- BIOS passwords
- Data/application encryption
- ***Hard drive encryption***
- ***Screen locking***
- ***Screen timeout***
- ***Security tokens***

5.2.5. The transmission of university data via infrared, bluetooth, 802.11x or other ***wireless*** technologies shall be in compliance with OSC Policy OSC-5, "Remote Access Security."

5.2.6. Regular system and data back-ups will be preformed as frequently as needed based on the risk assessment of the information maintained on the portable device, in accordance with OSC Policy OSC-3, "Information Security Framework." Back-ups shall be safeguarded and retained for a period commensurate with the value and criticality of the information.

5.2.7. University-owned Devices. OSC will provide designated personnel a computer to assist in the completion of their duties. At the end of their employment or association with OSC, or no longer need the equipment to carry out their duty, all equipment will be returned to the supervisor or designate.

5.2.8. Personal software and data is allowed on the computer system, as long as the software or data is legally owned or controlled by the user.

5.2.9. When a device is removed from service, OSC shall sanitize the IT equipment to remove information.

5.2.10. Privately-owned Devices. All OSC owned or licensed data or software on a personal owned or contractor-owned portable computing devices shall be removed, or recovered when no longer used or when the user's employment or contract terminates or when the portable computing device is no longer authorized for official OSC business.

5.2.11. ***Data Synchronization*** (Syncing). OSC has no legal liability for the loss of non-OSC data or the confidentially of data synchronized (synced) to university-owned or operated devices.

5.3. ***Identification and Authentication (I&A)*** Control. Portable computing devices shall accommodate I&A controls in accordance with OSC Policy OSC-8, "Password and PIN." If available, I&A controls shall be used to prevent unauthorized modifications of system settings.

5.4. Internet Connectivity. Portable computing devices connected to the Internet shall be in compliance with Ohio IT Policy ITP-B.6, "Internet Security," and OSC Policy, OSC-5, "Remote Access Security." At a minimum, 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. Inventory and Audit. OSC shall conduct inventory and security audits of portable computing devices on a regular and random basis.

5.6. Lost and Stolen Devices. In the event of a lost or stolen device, the person responsible for the equipment, including contractor and personal owned equipment with state software or data, shall notify their immediate supervisor or contract manager, and the OSC IT security contact within 1 business day. Information required in the report includes:

5.6.1. Date of loss, OSC data on the device and its sensitivity level, security on the device (encrpption levels) and other details relevant to the loss.

5.7. Privately-Owned and Contractor-Owned Portable Computing Devices. Privately-owned or contractor-owned devices are authorized for official university use. A privately-owned or contractor-owned portable computing device is used, the device shall meet the following additional requirements:

5.7.1. The device owner or contractor is responsible for obtaining, installing and maintaining malicious code security software in compliance with OSC Policy, OSC - 4, "Malicious Code Security."

5.7.2. The device owner or contractor is responsible for obtaining, installing and maintaining personal firewalls in compliance with Ohio IT Policy ITP-B.2, "Boundary Security."

5.7.3. OSC accepts no liability for the safeguarding or maintenance of non-university or non-OSC data on portable computing devices used in support of official OSC business or while acting as an agent of OSC. The users of privately-owned devices used for OSC work shall not have any expectation of personal privacy regarding the device and that such devices may be confiscated as evidence in civil or criminal proceedings.

5.7.4. No network access certification is needed.

6. References

6.1. 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.

6.2. Ohio IT Policy ITP-B.1, "Information Security Framework," is the overarching security policy for state information and services. Ohio IT Policy ITP-B.9, "Portable Computing Security," 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.

6.3. 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 communications. Unauthorized users must be detected and denied access.

6.4. 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.

6.5. Ohio IT Policy ITP-B.4, "Malicious Code," requires state agencies to implement and operate a malicious code security program. The program should help to ensure that adequate protective measures are in place against introduction of malicious code into state-controlled information systems and that computer system users are able to maintain a high degree of malicious code awareness.

6.6. Ohio IT Policy ITP-B.5, "Remote Access," requires state agencies to implement and operate security measures wherever a remote access capability is provided to state systems so that inherent vulnerabilities in such services may be compensated.

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

6.8. 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.

6.9. Ohio IT Policy ITP-E.1, "Disposal, Servicing and Transfer of IT Equipment," establishes agency requirements for the disposal, servicing or transfer of state agency IT equipment with regard to state data, licensed software and intellectual property, and rechargeable batteries and other hazardous materials.

6.10. 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.

7. Procedures

None.

8. Implementation

This policy is effective immediately.

9. Revision History

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

10. Definitions

Administrator Privileges. Ability to modify computer system settings, including access permissions associated with computer resources and data.

Computer Media. Computer readable or writeable permanent or temporary storage, such as CDs, DVDs, flash memory cards and diskettes.

Data. Coded representation of quantities, objects and actions. The word, "data," is often used interchangeably with the word, "information," in common usage and in this policy.

Data Synchronization (Syncing). The practice of updating data on two systems so that the data sets are identical.

Disk Drives. Magnetic and optical devices used by a computer to store and obtain data. Examples include hard drives, floppy disks, diskettes, CDs and DVDs.

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.

Identification and Authentication (I&A). 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 requesting 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.

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.

Portable Computing Device. Computer or device designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices.

Screen Locking. Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.

Screen Timeout. Mechanism to turn off a device or end a session when the device has not been used for a specified time period.

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

Service Level Agreement. Defines the services to be delivered, technical support and other parameters that, by contract, a business or supporting activity is required to deliver. The service level agreement should describe performance measures as well as penalties for failure to perform in

accordance with the service level agreement.

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."

Terms and Conditions. Language included in a contract that describes limits and expectations related to performance under the contract.

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 computer and telecommunication systems on behalf of the state.

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.

11. **Related Resources**

12. 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