Ohio Supercomputer Center

OSC Media Inventory Management

No:
OSC-2

Effective:
May 1, 2009

Issued By:
Kevin Wohlever
Director of Supercomputer Operations
Published By:
Ohio Supercomputer Center
Original Publication Date:
April 8, 2009

1. General Statement

The Ohio Supercomputer Center (OSC) community data is a valuable resource that must be maintained and protected. The purpose of this policy and accompanying procedures and resources is to help ensure the protection of the media containing the data from accidental or intentional unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use the data.

2. Supporting Documents: Procedures and Resources

OSC standards, policies and procedures are based on the standards of The Ohio State University, modified as needed for local requirements. The OSU policies can be found at: http://www.osu.edu/policies/

3. Scope and Applicability

This policy applies to all media that will be used with OSC computing systems as well as systems that access data from OSC storage environments. The policy applies regardless of environment, media, or device, where the data resides, is used and regardless of how the data may be transmitted.

4. Policy Statements and Procedures

4.1. Media Access Policy

OSC restricts access to storage media on computing systems to OSC authorized individuals

4.1.1. Media Access Procedures

4.1.1.1. Disks can be temporarily attached (for as long as it takes to transfer) to OSC systems or to systems on the OSC network to facility data transfer to/from OSC storage media. These devices will be returned to the provider.

4.2. Media Labeling

OSC affixes external labels to removable information system media and information system output.

4.2.1. Media Labeling Procedures

4.2.1.1. All tapes will be labeled externally with a label that has a bar code for machine readable, as well as human readable.

4.2.1.2. Because any tape can contain any number of users data, all tapes are considered to contain restricted data. No special marking is needed to reflect this designation

4.3. Media Storage

OSC controls physical access and securely stores information system media within a controlled area.

4.3.1. Media Storage Procedures

4.3.1.1. All storage attached to OSC systems will be kept in OSC secured computer rooms and locations.

4.3.1.2. OSC will not accept disk for permanent inclusion on its systems from outside (non-OSC) organizations.

4.3.1.3. Tape media will not be accepted from outside organizations for inclusion in the OSC tape management or library system.

4.4. Media Transport

OSC protects and controls information system media and restricts activities with transport of such media to authorized personnel.

4.4.1. Media Transport Procedures

4.4.1.1. OSC will not transport OSC storage media outside of its computer room(s).

4.4.1.2. Transportation of user data will be done on user provided storage media, and the user accepts all responsibility for the security of the media.

4.5. Media Sanitization

OSC sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

4.5.1. Media Sanitization Procedures

4.5.1.1. Disk storage devices that are still usable, but not of value to OSC will be made available for surplus. Before these disks are moved to surplus, they will be scrubbed (0s and 1s written in a random pattern) seven times before the media is released. If a scrubbing program cannot be run, the disks will be kept and destroyed.

4.5.1.2. All tapes will be degaussed before being sent to surplus or destroyed.

4.6. Media Disposal

OSC will destroy information system digital media that cannot be sanitized prior to disposal.

4.6.1. Media Disposal Procedures

4.6.1.1. When OSC storage disks are replaced due to failure, the replaced disk will be kept on site until it is destroyed. A failed disk will not be reused.

4.6.1.2. Tapes will be sanitized and then destroyed.

4.6.1.3. Certification of destruction will be controlled by serial number or tape ID label information.

5. Enforcement

OSC employees who violate this policy may be subject to penalties and disciplinary action both within and outside of the university. Alleged violations will normally be handled through the university disciplinary procedures applicable to the alleged violator. Violations of this policy will be reported to OSC management and may result in temporary or permanent denial of access to systems, media and / or facilities.

In a perceived emergency situation, OSC staff may take immediate steps including denial of access to the network, as well as seizure and quarantine of university-owned processing and storage assets to ensure the integrity of data and systems or protect OSC and the university from liability.

6.0 Procedures

None.

7.0 Implementation

This policy is effective immediately.

8.0 Revision History

Date	Description of Change
5/1/2009	Original policy.

9.0 Definitions

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