# Ohio Supercomputer Center Virtual Machine Lifecycle Management	**No:** **OSC-14**
	Effective: **May 1, 2011**
	Issued By: Kevin Wohlever Director of Supercomputer Operations **Published By:** Ohio Supercomputer Center **Original Publication Date:** May 17, 2011

1. General Statement

Virtual Machines at the Ohio Supercomputer Center (OSC) are a resource that must be maintained and protected. Hosting and maintaining all systems and virtual environment infrastructure requires support from a limited resource. The following policy and accompanying procedures and resources have been developed to reduce system management overhead and the impact on other users of OSC systems.

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/supercomputing/policies/

3. Scope and Applicability

This policy applies to all OSC users that use OSC resources to host software, web pages and portals on OSC systems. The policy applies by default and can be superseded by agreement between user communities and OSC or at the discretion of OSC management.

4. Policy Statements and Procedures

4.1. OSC Virtual System Policy

OSC virtual systems are made available to authorized users of OSC systems.

4.1.1. OSC will provide virtual systems for OSC staff development, user software testing and some production services.
4.1.2. OSC has the right to disable a virtual system that violates the acceptable use policies of OSC, The Ohio State University or the State of Ohio
4.1.3. OSC will provide VMs for a limited number of operating system environments.
4.1.3.1. The OSC supported VM environments will be listed on the OSC web site
4.1.3.1.1. Currently support VM environments
4.1.3.1.1.1. Microsoft Server
4.1.3.1.1.2. Microsoft Desktop

4.1.3.1.1.3. Red Hat Linux

4.1.4. OSC has the right to update the underlying OS or make appropriate configuration modifications to ensure system security

4.1.5. OSC has the right to disable a virtual system that poses a security risk to the OSC environment

4.1.6. OSC can monitor and charge for use of OSC systems

4.1.7. OSC can monitor user data movement to and from OSC systems

4.1.8. OSC staff will contact users about abnormal data storage use and / or data movement

4.1.9. OSC staff will not look at data stored in user storage areas unless required to maintain proper system functionality or authorized by the user.

4.1.10. OSC staff with authorized access to view user data will follow OSU data access and management policies

4.1.11. OSC does provide basic backup and recovery services for virtual systems.

4.1.12. OSC does not provide business continuity and disaster recovery services of virtual system services at this time.

4.2. OSC Virtual System Procedures

4.2.1. A virtual system request by an OSC staff member must be filed with the HPC services group.

4.2.1.1. A ticket for the service must be opened in the OSC service-now system

4.2.1.2. OSC can grant support for a virtual system for 6 months

4.2.1.2.1. An extension of 6 months can be granted

4.2.1.3. All virtual systems will be reviewed every six months.

4.2.1.3.1. If the system is not being used, it will be removed

4.2.1.3.2. If the system is still being used, an OS update may be required

4.2.2. A virtual system request by an OSC user must be filed with the OSC user services group

4.2.2.1. A ticket for the service must be opened in the OSC service-now system

4.2.2.2. OSC can grant support for a virtual system immediately for up to 6 months

4.2.2.3. SUG must review and approve a virtual machine request that will last longer than 6 months

4.2.2.3.1. An extension of 6 months can be granted by OSC staff

4.2.2.4. All virtual systems will be reviewed every six months.

4.2.2.4.1. If the system is not being used, it will be removed

4.2.2.5. If the system is being used, an OS update may be required

4.2.3. Virtual System Business Continuity and Disaster Recovery Services

4.2.3.1. (Future Placeholder) OSC plans to provide these services at some time in the future. …

5. Enforcement

OSC Users 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 or systems 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
5/17/2011	Original policy.

9.0 Definitions

10.0 Related Resources

Document Name

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