**Virtual Server Security Procedure**

# PurposeThe purpose of this procedure is to communicate standards for the secure configuration of virtual servers and hosts owned and/or operated by the [Organization].

# Scope

# This procedure applies to virtual server hosts that are owned, operated, or leased by [Organization]. All staff, employees and entities working on behalf of [Organization] are subject to this procedure.

# Procedure

The following restrictions should be enforced for all hypervisor hosts and guest virtual machines (VM.)

Administrator Access and Separation of Duties
Provide only server admins with on/off rights for their servers.

Network Security
The following requirements pertain to the physical network security of the Host servers:

* Disconnect all unused NICs from the physical host server.
* All network traffic between clients and hosts, between management systems and the hypervisor, and between the hypervisor and hosts are encrypted using SSL.
* Self-signed certificates are prohibited.
* All virtual switches will be in promiscuous mode for monitoring purposes.
* Enable and configure MAC address filtering to prevent MAC spoofing attacks.

Network Storage (all protocols)

* iSCSI and NFS should be placed on dedicated storage networks or non-routable VLANs to isolate data storage traffic from non-storage traffic.
* Enable and configure Challenge Handshake Authentication Protocol (CHAP) on all iSCSI connections prior to granting access.
* Use physical switches to detect and disallow IP or MAC address spoofing when using iSCSI or NFS.
* NFS: Configure the NFS server to restrict access to specific IP addresses related to your hypervisors.
* NFS: Use IPSec to secure traffic between the NFS server(s) and the hypervisors.
* Enable and configure Fibre Channel zoning to control access at the switch level.

Auditing and Logging

* Host logging is captured and transferred securely to a centralized location to track guest O/S online status, power events, hardware configuration changes, login events related to elevated privileges and Virtual Machine (VM) movement.
* Audit files should be read only and should only be read by authorized staff to ensure forensic integrity.
* Technical Services will conduct semi-annual audits of the environment including the virtual network, storage, the hypervisor, the VMs and the management systems.
* VMs will not be placed on storage, backup or management networks that are dedicated to the hypervisor.
* Disable screensavers.
* VMs will be configured so as to have no access or view to the resources used by the kernel or host.
* Technical Services should maintain a log of all running VMs.
* Unused VMs should be powered off.
* Unused hardware ports should be disabled.
* Enable guest access to physical devices on the host on an as-needed basis.
* Employ the use of VLANs within a single vswitch to segment traffic.
* Isolate VM motion traffic from the production network to an isolated segment that is non-routable and configured with a separate vswitch or VLAN.
* VMs should be configured so as to not directly access a VM data store or repository.
* Access to dormant VMs is restricted to the Operations staff.
* VMs should be created from an authorized template only.
* Validate the guest operating system update levels monthly.
* Disable all copy-paste functionality between hypervisor and VM.

Management Systems

* Communication between management systems and the hosts should be via secure, encrypted links.
* Limit workstation access to the hypervisor management server to authorized staff only.

Guest Operating Systems

* Virtual Machine (VM) operating systems must be supported by both the operating system vendor and the hypervisor that they are running on.
* All virtual servers must receive applicable security updates within 60 days of their release.
* VM templates must also receive Microsoft or other applicable software updates on a monthly basis.

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

The **[Department]** will verify compliance to this procedure through various methods, including but not limited to: periodic walk-throughs, business tool reports, internal and external audits, and feedback to the procedure owner.

# Exceptions

Limited exceptions to the procedure must be approved by the **[management]**.

1. **Definitions**
* Not applicable at this time