Virtual Server Security Procedure

1. Purpose

The purpose of this procedure is to communicate standards for the secure configuration of virtual servers and hosts owned and/or operated by The San Diego County Office of Education (SDCOE).

2. Scope

This procedure applies to virtual servers and virtual server hosts that are owned, operated, or leased by SDCOE. All employees, contractors, consultants, temporary and other workers at SDCOE must adhere to this procedure.

3. Procedures

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

Administrator Access and Separation of Duties

- Provide server admins with on/off rights for their servers only and no others.

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 to track guest O/S online status, power events, hardware configuration changes, login events related to elevated privileges and 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.

- Virtual Machine Security

- 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 shall maintain a log of all running VMs.

- Unused VMs shall be powered off.

- Unused hardware ports shall 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 shall 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 shall 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

- Communications between management systems and the hosts shall be via secure, encrypted links.

- Limit workstation access to the hypervisor management server to authorized staff only.

Guest operating systems
- Virtual Machine operating systems must be supported by both the operating system vendor and the hypervisor that they are running on.

- All virtual servers must be receive applicable security updates within 60 days of their release.

- Virtual Machine templates must also receive Microsoft or other applicable software updates on a monthly basis.

4. Compliance

Technical Services will verify compliance to this procedure through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the procedure owner.

5. Exceptions

All exceptions to this procedure must be approved by the ITS Assistant Superintendent.

6. Non-Compliance

Failure to comply with this Virtual Server Security Procedure may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

7. Related Procedures

- ITS Decommissioning Procedure
- SDCOE password Procedure

8. Revision History

Date of Change	Responsible	Summary of Change