Salisbury University

Virtualization Security Policy

1. PURPOSE

Organizations, including government agencies, are increasingly virtualizing servers and desktops to gain efficiency. The State's use of **virtualization** technology creates security challenges that must be addressed when deploying, migrating, administering, and retiring virtual machines. The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, managing the confidentiality, integrity, and availability of the Salisbury University (SU) networks, systems, applications, and data.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
8/26/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all official SUIT supported usage of virtualization technologies, such as server and desktop virtualization, will ensure risks to data loss or compromise are mitigated by operating in accordance with the requirements described in section 5.0 below.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

Salisbury University strives to implement efficient business processes and cost-beneficial technology solutions to provide the best possible services. Virtualization technologies are increasingly being used as an industry standard in order to gain operational efficiency. Virtualization offers the ability to streamline business functions using existing or new hardware purchases.

Virtualization also adds layers of technology which can create vulnerabilities and requires additional security controls to mitigate the ability to exploit weaknesses.

This policy applies to all **Full Virtualization** capabilities, whether:

- **Native Virtualization**; or
- **Hosted Virtualization**.

The requirements described below define the following security control areas that apply to virtualization:

- Identify and control how **confidential data** is, or may be, accessed, modified, or stored through a virtual environment
- Ensure accountability through authentication controls
- Ensure virtualized solutions are accounted for per the SU Asset Management Policy.
- Utilize tools to monitor for malicious activity and to help prevent data loss or compromise where possible.

If all four of these capabilities cannot be enabled, agencies should not deploy virtualized environments or assets with the ability to access any confidential information.

5.1 General Requirement for Dedicated Hardware Hosts

All hardware in a full-virtualization environment should be dedicated to the virtualization with only virtual implementations allowed; no non-virtual systems or applications will be allowed to share the virtualization host. The host should be configured to meet the security requirements of the highest security classification of all its supported guests wherever possible.

5.2 Hypervisor Security

Agencies handle a variety of data with varying classification levels requiring different security controls. Substantial security risks can be incurred when consolidating multiple services or data stores with differing classification levels within a single hypervisor. Therefore, as with securing a host, the hypervisor must also be configured where possible to meet the security requirements of the highest security-classification guest.

Generally, the hypervisor should be secured using the same methods as those used to protect software running on servers. Because of the hypervisor's level of access to and control over **guest OSs**, implementing security controls on the hypervisor helps prevent confidential data loss and limits the ability of an adversary to take control of *all* the guests.

Access to the virtualization management system should be restricted to authorized administrators only. It is important to secure each hypervisor management interface, both locally and remotely, and to restrict remote administration interfaces through the firewall. Depending on the specific hypervisor utilized by SUIT some of the

controls may not be applicable or feasible. Wherever possible, the detailed security controls related to hypervisor security listed in the table below should be implemented:

#	Name	Requirement
A	Patch Management	Install all updates to the hypervisor that are released by the vendor. Use centralized patch management solutions to administer updates, where applicable.
B	Restrict Access	Restrict administrative access to the management interfaces of the hypervisor Follow all the security policies for access control, authentication, elevated privilege, and least privilege as for any hardware-based system
C	Encrypt Communication	Protect all management communication channels by either method below: Use a dedicated management network ▪ Authenticate and encrypt management network communications
D	Asset Management	Create, deploy, and manage virtual machines (VMs) in accordance with the *Asset Management Policy*.
E	Configuration	Hypervisor should be secured where possible to the level of classification required by the highest-requirement guest OS.
F	Configuration Management	Centralize configuration management of hypervisors and follow configuration management processes to ensure that all configurations are documented.
G	Synchronization	Synchronize the virtualized infrastructure to a trusted authoritative time server.
H	Disconnect Unused Hardware	Disconnect unused physical hardware from the host system.
I	Disable Unneeded Services	Disable all hypervisor services, such as clipboards – or file sharing between the guest OS and the **host operating system (host OS)** – unless they are needed.
J	Monitoring Capabilities	Where possible, monitor the security indicators of: Each guest OS ▪ Activity occurring between guest OSs
K	Test and Production Environment	Separate production from test environments. Every host should be designated as belonging to either a production or the test environment, and all “work” on every host should maintain that separation.
L	Monitor Hypervisor	Carefully monitor the hypervisor itself for signs of compromise. This may include: ▪ Using self-integrity monitoring capabilities that hypervisors may provide ▪ Monitoring and analyzing hypervisor logs on an ongoing basis

5.3 Guest OS Security

The operating system of a virtual machine instantiated on a virtual server (i.e., a hypervisor) is referred to as a "guest" OS. All the security considerations that apply to OSs running on real hardware also apply to guest OSs; however, there are some additional security considerations. Agencies must apply and enforce the controls listed in the table below where applicable to ensure that guest OSs meet security configuration requirements and do not increase the risk of compromise for fellow guests.

#	Name	Requirement
A	Policy Application	Follow all recommended practices in SU Cybersecurity Policies for managing physical OSs, including but not limited to: ▪ Log management ▪ Authentication requirements ▪ Remote access controls
B	Configuration	No guest OS shall be secured at a higher security classification than its hypervisor.
C	Configuration Management	Centralize configuration management of guest OSs through the use of baseline template images for deployment and document configuration processes for deviations from the baseline where possible.
D	Patch Updates	Install all patch updates to the guest OS promptly, according to the *SU Patch Management Policy* and processes.
E	Backups	Back up all the virtual drives used by the guest OS on a regular schedule, using the same process for backups as is used for non-virtualized computers in the organization (See *Contingency Planning Policy*).
F	Disconnect Unused Hardware	Disconnect unused virtual hardware in each guest OS where possible.
G	Authentication Methods	Use separate local authentication credentials for each guest OS unless there is a particular reason for two guest OSs to share the same local authentication credentials.
H	Association	Ensure that virtual devices for the guest OS are associated only with the appropriate physical devices on the host system, such as the mapping between virtual network interface cards (NICs) to the proper physical NICs.
I	Compromised Systems	Investigate each guest OS for compromise during normal scanning for vulnerabilities.
J	Monitoring of Communication	Monitor the security of activity occurring between guest OSs where possible.

5.4 Secure Virtualization Planning & Deployment

The security of a virtual environment should be factored into the entire system development lifecycle, from planning to deployment, to maximize effective security and minimize the cost of security.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Confidential Information	Confidential information is non-public information and is defined by 2 subcategories: (1) Personally Identifiable Information; (2) Restricted Information. More information regarding Confidential Data can be found in the *SU Public and Confidential Information Policy*.
Full-virtualization	A form of virtualization where one or more operating systems and the applications they contain are run on top of virtualized hardware. There are two main types: (1) Native (or bare-metal) virtualization (2) Hosted virtualization
Guest Operating System (Guest OS)	A virtual guest or virtual machine (VM) that is installed under the host operating system.
Host Operating System	In a hosted virtualization solution, the OS that the hypervisor runs on top of.
Hosted Virtualization	A form of full virtualization where the hypervisor runs on top of a host OS.
Hypervisor	Also known as a Virtual Machine Monitor. The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.
Native Virtualization	Also known as a Bare-Metal Virtualization. A form of full virtualization where the hypervisor runs directly on the underlying hardware, without a host OS.
Operating System (OS)	A system software that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.
Virtualization	The simulation of the software and/or hardware upon which other software runs.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements

that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.