VMWare Hypervisor Configuration Standard

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 Virtualisation Standards 4

3. Standard Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Distribution 8

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

Virtual servers create a layer of abstraction that is of security concern and poses risk and requires additional mitigation to be in place. A major concern is the proliferation of virtual machines and stored VM images.

The objective of this standard is to ensure basic security consideration in virtual server environments/implementations includes physical security, application, database, anti-malware, access controls, patch management and monitoring

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* Security Technical Implementation Guides (STIGs): http://iase.disa.mil/stigs

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Virtualisation Standards

#### **Physical Segregation**

1. Hypervisor management shall be physically isolated from host and Virtual Machines (VM) access. Each host server should contain at least two physical Network Interface Cards (NICs). This NIC should be added to a network segment with an access list restricting access to only those devices/users directly responsible for maintaining the hypervisor and for VM creation and suspension.

#### **Logical Segregation**

1. Management access to virtual machines shall be granted based on a role-based model. Host access to administrator VMs and VM management access shall be segregated. Different password must be set for each VM. The use of single password across VMs is prohibited. Access to VM and management platform shall be restricted to only those directly responsible for maintaining the virtual environment.

#### **Securing and Patching VMs**

1. Anti-malware shall be installed on VM implementations and all unused ports should be closed. VMs should be installed with latest patch from the OEM and hardened by setting the baseline configuration across each VM. Data on VM should be of the same classification, different data classification should not be mixed on the same VM.

#### **Monitoring and Responding to Events**

1. Group VMs according to data classification. Ensure monitoring tools see packets internal to VMs managed by the same hypervisor. Segment Virtual networks and ensure VLANs are configured to isolate sets of VMs on the same host and across hosts. Ensure all VMs and host systems sync with time server for forensics and auditing purposes. Track all MAC addresses during VM initialization and moves. Ensure current snapshots exist to facilitate quick recovery during or after a business continuity event.

#### **Managing Change**

1. Uncontrolled proliferation of VMs is prohibited. Configuration of new VMs shall be subject to Change Management Board approval. Final image of a production server should be stored safely where it can provide quick path to recovery. Update the stored image each time you make change to the production instance.
2. Secure VM files. Ensure all files associated with running or stored VMs are kept in safe custody. Only authorized IT Staff directly responsible for VM file management or instantiation should have access to the VMs.

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Check the implementation settings on VM | * Confirm if the standard was implemented on the configurations |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Glossary / Acronyms

|  |  |
| --- | --- |
| VM | Virtual Machine |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* *Information Security*
* *IT Department*