Security Standard - Hypervisor (SS-009)

Chief Security Office

Date: 27/04/2023

Department for Work & Pensions

This Hypervisor Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-standards.

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision History

Version	Author	Description	Date
1.0		First published version	26/06/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls • Added NIST CSF references 11.1.1 Type 1 hypervisor by default 11.1.3 MLE mandated 11.2.1 Admins bypass faulty drivers 11.2.6 Device driver measure added 11.2.7 & 11.2.8 ACL measures added 11.2.9 VM image file encryption measure added 11.2.10 Server access protocol measure added 11.3.1 Removed prescriptive memory ratio 11.3.5 AV update measures added 11.3.7 Config measures added 11.3.8 VM image compliance measure added 11.3.9 Digital signature measure added 11.3.10 Resource limit measures added 11.4.10 Logging measures added	27/04/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	27/04/2023

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by first-line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. I].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

In this document the term **"must"** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications.

7. Accessibility Statement

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

A hypervisor is a software or hardware component of virtualisation that generates, controls, and executes virtual machines. It is also referred to as a virtual machine monitor/manager (VMM).

Hypervisors are classified into two types, "Type 1" and "Type 2". A type 1 hypervisor is a native or bare-metal hypervisor. In this configuration, there is no host OS, instead, the hypervisor installs directly onto the hardware where the host OS would normally reside. A type 2 hypervisor functions as a software layer on top of an operating system, much like other computer programs.

The implementation of hypervisors allows for greater versatility, performance, accessibility and speed.
This Hypervisor Security Standard defines the minimum technical security measures that **must** be implemented for use within the Authority.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls v8 controls set. [see Appendix C External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to hypervisors are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with hypervisors, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF), and are enabled by the implementation of controls from the CIS Critical Security Controls v8 controls set. [see Appendix C External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

This standard applies to all hypervisor deployments within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

Due to hypervisors being an essential component of virtualisation, many statements throughout this document will refer to virtual machines. Please also refer to SS-025 Virtualisation Security Standard for specific standards.

11. Minimum Technical Security Measures

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1 Hypervisor Platform Architectural Choices

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	There **must** be consideration of which type of hypervisor would be most suitable for the Authority's need. A Type 1 hypervisor provides more security assurance than a Type 2 hypervisor, due to the reduced attack surface (given the absence of Host O/S) and the consequent reduced list of vulnerabilities to be addressed. A Type 1 hypervisor **must** be used by default, and Type 2 only where necessary.	PR.DS-1 PR.DS-5
11.1.2	There **must** be a consideration for the platform virtualisation approach that would be most suitable for the Authority's needs. For example, a hypervisor platform with hardware assisted virtualisation (both instruction set and memory management) provides greater security assurance than one with purely software assisted virtualisation.	PR.DS-1 PR.DS-5
11.1.3	The hypervisor that is launched **must** be part of a platform and an overall infrastructure that contains hardware supporting a **Measured Launch System (MLE)** such as a Trusted Platform Module (TPM v2.0 or later), with the means to provide an attestation process and chain of trust.	PR.DS-1 PR.DS-5

11.2 Device Emulation & Access Control

The following security measures **must** be in accordance with SS001-1 Access & Authentication [Ref. F] and SS001-2 Privileged User Access Security Standards [Ref. G] where appropriate.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	The hypervisor **must** have a boot configuration choice to disallow the user of non-certified drivers. Further, if architecture permits, the running of QEMU process or each application VM should be confined to an unprivileged VM so as to limit the impact of a faulty device driver code to the operation of the corresponding application VM. Administrators **must** be able to bypass faulty drivers if necessary.	PR.DS-1 PR.DS-5
11.2.2	The access control solution for VM administration **must** have the granular capability both at the permission assignment level as well as at the object level (i.e., the specification of the target of the permission can be a single VM or any logical grouping of VMs – based on function or location).	PR.AC-4
11.2.3	The access control solution for VM administration **must** have the ability to deny permission to some specific objects within a VM group (e.g., VMs running workloads of a particular sensitivity level) in spite of having access permission to the VM group.	PR.AC-4
11.2.4	The number of user accounts (including privileged accounts) requiring direct access to hypervisor host **must** be limited to only those that are absolutely necessary.	PR.AC-4
11.2.5	Access to the hypervisor **must** be restricted according to least privilege and need to know basis.	PR.AC-4
11.2.6	Device drivers that are deployed as part of a hypervisor platform, **must** be set up to operate in user mode or a process with lower privileges, rather than on par with the privilege level of the hypervisor or kernel mode.	PR.AC-4 PR.PT-3
11.2.7	A configured Access Control List (ACL) **must** be in place to restrict each VM process's access to only the devices assigned to that VM.	PR.AC-4 PR.AC-5 PR.PT-3
11.2.8	A strong access control system **must** be used to enforce restrictions on which administrators are allowed to check images into and out of the VM Image library.	PR.AC-1 PR.AC-4

11.2.9	VM image files **must** be kept in encrypted devices that can only be opened or closed by a select group of authorised administrators with passphrases of adequate complexity if there is no access control mechanism.	PR.DS-1 PR.AC-4
11.2.10	Access to servers that store VM images **must** always be via a secure protocol such as TLS.	PR.DS-2

11.3 VM Management

The following security measures are included to ensure performance is maximised, VM conflicts minimised, and to protect VM workloads, thus supporting availability requirements. As such they are included as advisory measures where appropriate, for consideration from a security perspective.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	The ratio of the combined configured memory of all VMs to the RAM memory of the virtualised host **must** be sufficient to provide acceptable performance and availability.	PR.DS-4
11.3.2	The hypervisor **must** have configuration options available to specify guaranteed physical RAM for every VM (that requires it) along with a limit to this value, and to specify a priority value for obtaining the required RAM resource in situations of contention among multiple VMs.	PR.DS-4
11.3.3	The number of virtual CPUs allocated to any VM deployed **must** be strictly less than the total number of cores in the hypervisor host.	PR.DS-4
11.3.4	The hypervisor **must** provide features to specify a lower and upper limit or CPU clock cycles needed for every deployed VM as well as a feature to specify a priority score for each VM, to facilitate scheduling in situations of contention for CPU resources from multiple VMs.	PR.DS-4
11.3.5	There **must** be a mechanism for security monitoring of a guest OS provided through introspection, and security policy enforcement of VM operations – malicious processes running inside VMs and malicious traffic going in and out of the VM. This monitoring and enforcement mechanism forms the foundation for building Anti-Virus (AV) and Intrusion Detection & Prevention (IDPS) solutions. All anti-malware tools running on the virtualised host (e.g. firewalls, anti-virus scanners, and IDPS) **must** be able to carry out autonomous signature or reference file updates on a regular basis.	DE.CM-4 DE.CM-7

11.3.6	Solutions for Security Monitoring and security policy enforcement of VMs **must** be compliant with SS-025 Virtualisation Security Standard [Ref. D].	DE.CM-7
11.3.7	VM configuration management tools **must** be able to compile logs and notify administrators when configuration changes are detected in any monitored VM.	PR.PT-1 DE.DP-4
11.3.8	All VMs images **must** adhere to SS-025 Virtualisation Security Standard, and any VM images that do not meet this standard **must** not be kept on the VM image server or in the VM image library.	PR.IP-3
11.3.9	As a mark of authenticity and integrity, every VM image kept in the image server **must** have a digital signature affixed to it that was created using reliable, strong cryptographic keys. This must be in accordance with SS-002 PKI & Key Management [Ref. H] and SS-007 Use of Cryptography Security Standards [Ref. B].	PR.DS-6
11.3.10	Resource limits **must** be implemented for network bandwidth and I/O bandwidth (e.g., CPU) for each VM to mitigate denial-of-service (DOS) attacks.	PR.PT-4

11.4 Administration of Hypervisor Host & Hypervisor Software

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	If possible, the user accounts (including privileged accounts) on the hypervisor host **must** be integrated with the enterprise directory infrastructure in order to enable authentication through robust authentication protocols (e.g., Kerberos), enable enforcement of some corporate security policies (e.g., password policies) as well as handle changes to user account list (addition and deletion of user accounts).	PR.AC-1 PR.AC-4
11.4.2	The use of administrative functions **must** be restricted to defined endpoint networks and devices, such as specific laptops or desktops that have been approved for such access.	PR.AC-4 PR.MA-1
11.4.3	Multi-factor authentication **must** be required for all administrative functions.	PR.AC-7

11.4.4	Administrative functions **must** be separate such that hypervisor administrators do not have the ability to modify, delete, or disable hypervisor audit logs.	PR.AC-4 PR.MA-1
11.4.5	Duties for administrative functions **must** be separate, such that authentication credentials for the hypervisor do not have access to applications, data, or individual virtual components.	PR.AC-4
11.4.6	The remote access protocol used to access the hypervisor service console **must** have configuration options available to; • completely deny access (i.e., disable remote access via specific protocols); • deny hypervisor root account access; • restrict access only to a specified list of administrative accounts.	PR.AC-3
11.4.7	Use Hypervisor features that enable: • Definition of a complete set of configuration settings (Gold Configuration) for a hypervisor deployment • Automate application of those configuration settings to a new or existing hypervisor installation and, Check compliance of existing hypervisor installation against those configuration settings, if available, in order to minimise manual configuration errors that may increase the security risk.	PR.IP-3
11.4.8	Hypervisor hosts and software **must** be patched with the most recent, secure, and satisfactorily tested code and must be in accordance with SS-033 Security Patching Standard [Ref. E]. Regular vulnerability management testing **must** also be conducted.	PR.DS-5 PR.IP-12
11.4.9	The built-in firewall for the hypervisor **must** only be configured to allow ports and protocols (network traffic) needed for enabled services in the hypervisor, such as management and specialised security agents and third-party applications.	PR.DS-2

11.4.10	The hypervisor **must** have a logging feature that generates logs in a standardised format (e.g., syslog as opposed to a proprietary format) to help leverage the use of tools with good analytical capabilities. Access to log data **must** be through a secure protocol (e.g., TLS 1.2), must be read only, and **must** be restricted only to those staff who require it. Safeguards **must** be in place to detect changes in logs, in accordance with SS-012 Protective Monitoring Security Standard. [Ref. A].	PR.DS-2 DE.AE-3
11.4.11	The configuration of a logging program in a hypervisor **must** be set up to store the log messages in an external server. This is critical since these messages may become inaccessible if the platform on which the hypervisor is resident is breached.	DE.AE-3
11.4.12	The Protection of VM Management and Hypervisor Host & Software administration functions **must** be ensured by placing the management interface of the hypervisor in a dedicated virtual network segment and enforcing traffic controls using a firewall (e.g. designating the subnets in the enterprise network from which incoming traffic into the management interface is allowed).	PR.PT-4
11.4.13	Communication from a given VM to the enterprise (physical) network **must** be enabled by establishing multiple communication paths within the virtualised host. This is usually accomplished by providing multiple physical network adapters for traffic from a particular VM to reach the enterprise network.	PR.PT-4

12 Appendices

Appendix A Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.2.8, 11.4.1
PR.AC-3	Remote access is managed	11.4.6
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.4.1, 11.4.2, 11.4.4, 11.4.5
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.2.7
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.4.3
PR.DS-1	Data-at-rest is protected	11.1.1, 11.1.2. 11.1.3, 11.2.1, 11.2.9
PR.DS-2	Data-in-transit is protected	11.2.10, 11.4.9, 11.4.10
PR.DS-4	Adequate capacity to ensure availability is maintained	11.3.1, 11.3.2, 11.3.3, 11.3.4,
PR.DS-5	Protections against data leaks are implemented	11.1.1, 11.1.2, 11.1.3, 11.2.1, 11.4.8, 11.4.8

PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.3.9
PR.IP-3	Configuration change control processes are in place	11.3.8, 11.4.7
PR.IP-12	A vulnerability management plan is developed and implemented	11.4.8
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.4.2, 11.4.4
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.3.7
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.2.6, 11.2.7
PR.PT-4	Communications and control networks are protected	11.3.10, 11.4.12, 11.4.13
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.4.10, 11.4.11
DE.CM-4	Malicious code is detected	11.3.5
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.3.5, 11.3.6
DE.DP-4	Event detection information is communicated	11.3.7

Appendix B Internal References

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 2 – Internal References

Ref	Document	Publicly Available*
A	SS-012 Protective Monitoring Security Standard	Yes
B	SS-007 Use of Cryptography Security Standard	Yes
C	Information Management Policy	Yes
D	SS-025 Virtualisation Security Standard	Yes
E	SS-033 Security Patching Standard	Yes
F	SS-001 pt.1 Access & Authentication Security Standard	Yes
G	SS-001 pt.2 Privileged User Access Security Standard	Yes
H	SS-002 PKI & Key Management Security Standard	Yes
I	Security Assurance Strategy	No

Requests to access non-publicly available documents **should be made to the Authority.*

Appendix C External References

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
NIST Cyber Security Framework
OWASP Open Web Application Security Project

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
AV	Anti-virus
CIS	Centre for Internet Security
COTS	Commercial Off The Shelf
CPU	Central Process Unit
CSF	Cyber Security Framework
DDA	Digital Design Authority
IDPS	Intrusion Detection & Prevention
NIST	National Institute for Standards and Technology
OWASP	Open Web Application Security Project
QEMU	Quick Emulator
RAM	Random Access Memory
VM	Virtual Machine

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Attestation	The process of confirming entitlement as it exists as present.
Clock Cycle	The amount of time between two pulses of an oscillator and determines the speed of a computer processor.
Full Virtualisation	A form of virtualisation which uses a hypervisor hardware platform with virtualisation extensions and hence supports Virtual Machines (VMs) with unmodified Guest O/Ss to run on them.
Hypervisor	A software built using the kernel of an O/S, along with supporting kernel modules that provides separation for various execution stacks represented by Virtual Machines.
Hypervisor Platform	The collective term for a hypervisor and its hardware host.
QEMU (Quick Emulator)	A software module that is a component of the hypervisor platform that supports full virtualisation by providing emulation of various hardware devices.
Security Virtual Appliance	A security tool that performs the function of monitoring and protecting Virtual Machines (VMs) run from a specially security hardened, independent VM
Type 1 Hypervisor	A hypervisor which is installed directly onto the hardware (also known as bare metal).
Type 2 Hypervisor	A hypervisor which requires an underlying O/S (called Host O/S).
Virtual Machine (VM)	A software-defined complete execution stack consisting of virtualised hardware, operating system, middleware and applications.

Virtualisation	A methodology for emulation or abstraction of hardware resources that enables complete execution stacks including software applications to run on it.
Virtualised Host	The physical host on which the virtualisation software such as the hypervisor is installed. Usually, the virtualised host will contain a special hardware platform that assists virtualisation – specifically Instruction Set and Memory virtualisation.

Appendix F Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps