Security Standard - Hypervisor (SS-009)

Chief Security Office

Department for Work & Pensions

Date: 20/05/2026

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	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

1. Contents

1. Contents **3**
2. Revision History **4**
3. Approval History **6**
4. Compliance **7**
5. Exceptions Process **7**
6. Audience **7**
7. Accessibility Statement **7**
8. Introduction **8**
9. Purpose **9**
10. Scope **9**
11.1 Hypervisor Platform Architectural Choices 10
11.2 Device Emulation & Access Control 12
11.3 VM Management 15
11.4 Administration of Hypervisor Host & Hypervisor Software 18
12 Appendices **24**
Appendix A Security Outcomes 24
Appendix B Internal References 26
Appendix C External References 26
Appendix D Abbreviations 27
Appendix E Definition of Terms 28
Appendix F Accessibility artefacts 29

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

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Intro – Threats Scope – Cloud service provider / Authority responsibilities 11.1.2 Hardware assisted virtualisation 11.1.3 Split CSP and Authority responsibilities 11.1.4 Backups; Split CSP and Authority responsibilities 11.2.5 & 11.2.8 Ref added to SS-001-2 11.2.9 Encryption requirements 11.2.10 Ref added to SS-007 11.2.11 Disable emulated hardware devices; Split CSP and Authority responsibilities 11.2.12 Disable data transfers 11.3.3 policy-driven oversubscription limits 11.3.5 Security monitoring; continuous 11.3.10 Resource allocation policies; resource exhaustion 11.3.11 EDR tools 11.4.1 Tiered admin model 11.4.2 PAWs; cloud-native controls 11.4.3 Ref added to SS-001-2	20/05/2026

		11.4.4 MFA; Dual authorisation 11.4.6 Disable root/admin accounts; changing passwords; break glass accounts; Split CSP and Authority responsibilities 11.4.7 Must 11.4.8 Scanning 11.4.9 Ref added to SS-013; Split CSP and Authority responsibilities 11.4.12 Split CSP and Authority responsibilities Internal references – SS-013 Firewall Security; SS-035 Backup & Recovery External References - NIST SP 800-125A Rev. 1 Definitions – On-premise; ILO	

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	27/04/2023
2.1		Chief Security Officer	20/05/2026

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

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

- controls tests performed by 1st 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, however due to their central management capabilities over many virtualised environments they can act as a 'force multiplier' allowing attackers to manage these environments, change configurations and access privileges, install malware or bypass controls.

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 NCSC, 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 set. [see 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 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. Please note that some security objectives have requirements that are split between the Cloud Service Provider and the Authority system owner.

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

(Important) this table contains '**must**' activities.

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 Department'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-05

<table>
<tr><td>11.1.2</td><td colspan="2">Use of hardware assisted virtualisation (both instruction set and memory management, specifically Second Level Address Translation (SLAT) and I/O Memory Management Units (IOMMU)) must be preferred over purely software assisted virtualisation to provide greater security assurance and meet the needs of the Department. See NIST SP 800-125A Rev. 1 [External references].</td><td>PR.DS-05</td></tr>
<tr><td rowspan="2">11.1.3</td><td colspan="2">For on-premise devices, where the Authority has control of the hypervisor host, the hypervisor that is launched must be part of a platform and an overall infrastructure that contains hardware supporting a <u>Measured Launch System (MLE)</u> such as a Trusted Platform Module (TPM v2.0 or later), with the means to provide an attestation process and chain of trust.
For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;</td><td rowspan="2">PR.DS-05</td></tr>
<tr><td>Cloud Service Provider:
- Measurements stored in Platform Configuration Registers sent to remote attestation server</td><td>Authority tenant controls:
- Verify attestation measurements
- Boot process; Static Root of Trust for Measurement (SRTM) or Dynamic Root of Trust for Measurement (DRTM).
- Confidential VMs</td></tr>
</table>

<table>
<tr><td rowspan="2">11.1.4</td><td colspan="2">For on-premise devices, where the Authority has control of the hypervisor host, immutable backups of hypervisor and VM configurations must be made in line with SS-035 Backup & Recovery security standard [Ref. K].
For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;</td><td rowspan="2">PR.DS-11</td></tr>
<tr><td>Cloud Service Provider:
- Hypervisor config</td><td>Authority tenant controls:
- Template/versioning of images
- Policy-as-Code in source control
- Immutable backup of state</td></tr>
</table>

11.2 Device Emulation & Access Control

(Important) this table contains '**must**' activities.

The following security measures **must** be in accordance with SS001-1 Access & Authentication [Ref. F] and SS-001-2 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.AA-05

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.AA-05
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.AA-05
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.AA-05
11.2.5	Access to the hypervisor **must** be restricted according to least privilege and need to know basis, in line with SS-001-2 Privileged User Access security standard [Ref. G].	PR.AA-05
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.AA-05
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.AA-02 PR.AA-05

<table>
<tr><td>11.2.8</td><td>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, in line with SS-001-2 Privileged User Access security standard [Ref. G].</td><td>PR.AA-02
PR.AA-05</td></tr>
<tr><td>11.2.9</td><td>All VM files containing sensitive Authority data must be kept on encrypted devices using hypervisor-native encryption or guest-level encryption managed by an enterprise Key Management Service (KMS), in accordance with SS-007 Use of Cryptography security standard [Ref. B], and 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.</td><td>PR.DS-01
PR.AA-02
PR.AA-05</td></tr>
<tr><td>11.2.10</td><td>Access to servers that store VM images must always be via a secure protocol such as TLS, in line with SS-007 Use of Cryptography security standard [Ref. B]</td><td>PR.AA-02
PR.DS-02</td></tr>
<tr><td>11.2.11</td><td>The hypervisor configuration must disable all emulated hardware devices not explicitly required for the function of the Guest VM (e.g. keyboards, mice, floppy drives, serial/parallel ports, USB controllers ILO management cards etc.);
For on-premise devices, where the Authority has control of the hypervisor host, these must be disabled at the BIOS/UEFI level of the VM where applicable.
For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;

Cloud Service Provider:
- Host-level hardening

Authority tenant controls:
- Virtual Private Cloud
- Network Security Groups</td><td>PR.PS-01
PR.IR-01</td></tr>
</table>

		- Security Groups - Identity & Access Management - Key Management Services - Guest OS configuration	
11.2.12	Data transfer mechanisms between the Guest VM and the hypervisor remote console (e.g., copy/paste, drag-and-drop, HGFS) **must** be disabled by default. Enabling these features requires a documented exception and risk assessment. See NIST SP 800-125 [External references].		PR.PS-01 PR.IR-01

11.3 VM Management

(Important) this table contains '**must**' activities.

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-10 PR.IR-04
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-10 PR.IR-04

11.3.3	The number of virtual CPUs allocated to any VM deployed **must** implement policy-driven oversubscription limits by workload class.	PR.DS-10 PR.IR-04
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-10 PR.IR-04
11.3.5	Security monitoring of guest OSs **must** be in place in line with SS-012 Protective Monitoring security standard [Ref. A] as a minimum, but in addition events such as malicious processes running inside VMs and malicious traffic going in and out of the VM, to enforce security policy of VM operations, **must** also be monitored. This may be provided by VM introspection but outputs **must** include details of telemetry coverage and prevention/detection activities. Monitoring and enforcement mechanisms form 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 continuous basis.	DE.CM-09
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-09
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.PS-04 DE.CM-09

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.PS-01
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-10
11.3.10	Resource limits (supported by resource allocation policies) **must** be implemented for network bandwidth and I/O bandwidth (e.g., CPU) for each VM to prevent resource exhaustion and mitigate denial-of-service (DOS) attacks.	PR.DS-10 PR.IR-04
11.3.11	Endpoint Detection and Response (EDR) / telemetry **must** be present and monitored to detect malicious events; at the hypervisor layer (where vendor-supported) for Type 2 hypervisors, or via supported platform telemetry and control-plane logs at the application/VM layer for Type 1 hypervisors.	DE.CM-09

11.4 Administration of Hypervisor Host & Hypervisor Software

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Hypervisor management authentication **must** utilise a Tiered Administration Model, in line with SS-001-2 Privileged User Access security standard [Ref. G]. Hypervisors **must** be treated as **Tier 0** assets, and administration accounts **must** be separate from standard user accounts and **must** be integrated with the enterprise directory infrastructure in order to enable authentication through robust authentication protocols (e.g. Kerberos), enable enforcement of corporate security policies (e.g. password policies) as well as handle changes to user account list (addition and deletion of user accounts).	PR.AA-03 PR.AA-05
11.4.2	For on-premise devices, where the Authority has control of the hypervisor host, the use of administrative functions **must** be restricted to trusted, hardened Privileged Access Workstations (PAWs). These devices **must** be logically or physically isolated from the general corporate network and **must** not have direct internet access or email clients installed. For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, other equivalent cloud-native controls **must** be implemented, such as zero trust controls.	PR.AA-05
11.4.3	Multi-factor authentication **must** be required for all administrative functions in line with SS-001-2 Privileged User Access security standard [Ref. G].	PR.AA-03

11.4.4	Administrative functions **must** employ MFA be separate such that hypervisor administrators do not have the ability to modify, delete, or disable hypervisor audit logs. Where feasible, dual authorisation **must** be in place to prevent a single administrator being able to make changes to the hypervisor's configuration that would create a vulnerability or actively exploit the access granted. Where this is not feasible this **must** be recorded in the appropriate risk register.	PR.AA-05
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.AA-04 PR.AA-05
11.4.6	For on-premise devices, where the Authority has control of the hypervisor host, 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. Default root/admin accounts **must** be disabled or secured with a complex password which **must** be changed on indication of compromise, in line with NCSC guidance and SS-001-1 Access & Authentication security standard [Ref. F].	PR.AA-02 PR.AA-04 PR.AA-05

<table>
<tr><td></td><td colspan="2">Emergency Access (e.g. "Break-Glass") accounts must be created, secured in a physical/digital vault, and monitored to alert immediately upon use.
For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;</td><td></td></tr>
<tr><td></td><td>Cloud Service Provider:
- Host-level hardening</td><td>Authority tenant controls:
- Virtual Private Cloud
- Network Security Groups
- Security Groups
- Identity & Access Management
- Key Management Services
- Guest OS configuration</td><td></td></tr>
<tr><td>11.4.7</td><td colspan="2">Hypervisor features must be used 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.</td><td>PR.PS-01</td></tr>
<tr><td>11.4.8</td><td colspan="2">Hypervisor hosts and software must be patched with the most recent and satisfactorily tested code and must be in accordance with SS-033 Security Patching Standard [Ref. E]. Regular vulnerability management scanning must also be conducted.</td><td>ID.AM-08
PR.PS-02</td></tr>
</table>

<table>
<tr><td>11.4.9</td><td colspan="2">For on-premise devices, where the Authority has control of the hypervisor host, the built-in firewall for the hypervisor (where applicable) 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. See SS-013 Firewall Security standard [Ref. J] for further information.

For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;</td><td>PR.IR-01</td></tr>
<tr><td></td><td>Cloud Service Provider:
- Host-level hardening</td><td>Authority tenant controls:
- Virtual Private Cloud
- Network Security Groups
- Security Groups
- Identity & Access Management
- Key Management Services
- Guest OS configuration</td><td></td></tr>
<tr><td>11.4.10</td><td colspan="2">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].</td><td>PR.AA-05
PR.DS-02
PR.PS-04
DE.CM-09</td></tr>
</table>

<table>
<tr><td>11.4.11</td><td colspan="2">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.</td><td>PR.DS-01
PR.PS-04</td></tr>
<tr><td>11.4.12</td><td colspan="2">For on-premise devices, where the Authority has control of the hypervisor host, 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).

For cloud-hosted hypervisors, where the Authority does not manage the underlying hypervisor, equivalent cloud-native controls must be implemented, such as;</td><td>PR.PS-01
PR.IR-01</td></tr>
<tr><td></td><td>Cloud Service Provider:
- Host-level hardening</td><td>Authority tenant controls:
- Virtual Private Cloud
- Network Security Groups
- Security Groups
- Identity & Access Management
- Key Management Services
- Guest OS configuration</td><td></td></tr>
</table>

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.IR-01 PR.IR-04

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
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.4.8
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.2.7, 11.2.8, 11.2.9, 11.2.10, 11.4.6
PR.AA-03	Users, services, and hardware are authenticated	11.4.1, 11.4.3
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.4.5, 11.4.6
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.2.1, 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, 11.4.6, 11.4.10

PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.2.9, 11.4.11
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.2.10, 11.4.10
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.1.1, 11.1.2, 11.1.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.9, 11.3.10
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.1.4
PR.PS-01	Configuration management practices are established and applied	11.2.11, 11.2.12, 11.3.8, 11.4.7, 11.4.12
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.4.8
PR.PS-04	Log records are generated and made available for continuous monitoring	11.3.7, 11.4.10, 11.4.11
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.2.11, 11.2.12, 11.4.9, 11.4.12, 11.4.13
PR.IR-04	Adequate resource capacity to ensure availability is maintained	11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.10, 11.4.13
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.3.5, 11.3.6, 11.3.7, 11.3.11, 11.4.1

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
J	SS-013 Firewall Security standard	Yes
K	SS-035 Backup & Recovery security standard	Yes

Requests to access non-publicly available documents **should be made 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 set
NIST Cyber Security Framework
OWASP Open Web Application Security Project
NIST SP 800-125A Rev. 1 Security Recommendations for Server-based Hypervisor Platforms

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.
Integrated Lights Out (ILO) management card	A dedicated, embedded processor and network interface that allows administrators to remotely monitor, manage, and troubleshoot servers, even when powered off or without an operating system.
On-premise	Locally installed software that runs on an organisation's own IT environment
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:

DWP Accessibility Policy
DWP Accessibility Manual
Guidance and tools for digital accessibility
Understanding accessibility requirements for public sector bodies