Security Standard - Virtualisation (SS-025)

Chief Security Office

Department for Work & Pensions

Date: 27/04/2023

This Virtualisation 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-and-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	17/07/17
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 • Inserted reference to Cloud Computing Standard for further direction for Cloud virtualisation (Scope) 11.1 Removed reference to asset register 11.1.3 Inactive images patched prior to reactivation 11.2 Added references to Gold Builds and immutability 11.3 Snapshot Management added 11.4 Amended changes 11.5 Amended changes 11.8 Amended changes 11.3 Section added on snapshot management 11.5.5 Backup requirement updated 11.5.6 Sanitisation requirement added. 11.6.2 Admin measures added 11.6.3 Compliance to SS-009 added 11.6.4 Admin access measures added 11.6.5 Authentication measures added 11.8.2 Time source added 11.8.8 Monitoring measures added 11.8.9 Anomaly detection measures added	27/04/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	17/07/17
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. M].
- 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

Virtualisation technology is used to create a virtual version of something, such as a storage device, server, operating system (OS), or network resources, as opposed to traditional bound hardware.

The capacity to launch individual instances of virtual servers or services on demand, running the precise OS version required for a given application, and real-time scalability are just a few of the benefits that virtualisation offers.

This Virtualisation 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 (see Appendix C for full list external references) 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 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 virtualisation are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with virtualisation, 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 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 deployments upon virtualised infrastructure (where there is hardware virtualisation) within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data. This includes virtual machines, virtual storage, and virtual networks.

This standard does not cover;

- Desktop Virtualisation (Thin Clients)
- Application Virtualisation (Containerisation)

Please refer to the SS-023 Cloud Computing Security Standard for virtualisation specific measures.

Due to hypervisors being an essential component of virtualisation, many statements throughout this document will refer to hypervisors. Please also refer to SS-009 Hypervisor Security Standard [Ref. G] for specific statements.

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

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 Governance

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	There **must** be controls in place to prevent unauthorised creation, destruction, or copying of virtual machines.	PR.IP-2 PR.IP-3
11.1.2	Virtual Machines **must** have business continuity and disaster recovery controls. VM's **must** be designed to be able to gradually degrade functionality, in the case of an incident that prohibits from maintaining full functionality.	PR.IP-9 PR.IP-10
11.1.3	Virtual machines, and virtual machine images **must** be patched (or updated) in line with SS-033 Security Patching Standard [Ref. A]. Any inactive images **must** be patched (or updated) before being put back into operation. Regular vulnerability management testing **must** also be conducted.	DE.CM-4 PR.IP-12
11.1.4	All virtualised software, including that which is automatically provisioned, **must** be correctly and appropriately licensed.	ID.AM-2
11.1.5	Testing **must** be performed to ensure that the network infrastructure, servers, and storage can support virtualisation.	PR.IP-5

11.2 Virtual Machine Images

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Live virtualised systems **must** be created from pre-configured, system images (VM Images), which can be referred to as Gold Builds. Once created, these images are immutable and cannot be changed – if a patch / update is required, a new version of the Gold Build **must** be created.	DE.CM-4
11.2.2	VM Images **must** be hardened in accordance with SS-008 Server Operating System Security Standard [Ref. B].	PR.DS-1 PR.DS-5
11.2.3	VM images **must** have controls in place to protect them from: • Malware • Unauthorised access • Unauthorised modification • Unauthorised deletion • Unauthorised copying	DE.CM-4 PR.AC-3 PR.DS-1

11.2.4	VM Images **must** be stored in a storage location logically separate from the storage location where inactive or dormant VMs are stored.	PR.DS-7
11.2.5	Measures **must** be in place to ensure images are periodically updated but to also prevent the proliferation of images, also known as sprawl.	PR.MA-1

11.3 Snapshot Management

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Consideration **must** be taken for snapshots as they can prove to be more of a risk compared to images. This is due to them containing contents of RAM memory which might include sensitive information.	PR.DS-1

11.4 Encryption

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Encryption implemented on Virtual Machines **must** assess the impacts virtualisation has on encryption and mitigate where this creates additional risks. This includes entropy exhaustion and side channel attacks.	PR.DS-1

11.5 Virtual Storage

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Access to virtual storage solutions **must** be restricted only to users and functions that require access to that storage.	PR.AC-4
11.5.2	Attempts to access virtual storage solutions **must** be authenticated prior to access being granted.	PR.AC-7
11.5.3	Encryption of virtual storage **must** be in accordance with SS-007 Use of Cryptography Security Standard [Ref. C] and SS-002 PKI & Key Management Security Standard [Ref. D] where appropriate.	PR.DS-1
11.5.4	Backups, archives, and copies of virtual storage **must** be securely stored commensurate with the security of the original source.	PR.DS-1

11.5.5	Backups of virtual drives **must** be conducted on a regular basis and **must** comply with the SS-035 Secure Backup and Recovery Security Standard [Ref. J].	PR.IP-4
11.5.6	Storage used in virtualised environments **must** be securely sanitised before being re-allocated or decommissioned and **must** comply with SS-036 Sanitisation and Destruction Security Standard [Ref. K].	PR.IP-6

11.5 Virtual Networking

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Standard network controls **must** be applied to virtualised networks as if they were physical networks, in compliance with SS-018 Network Security Design Security Standard [Ref. E].	PR.PT-4
11.5.2	Management networks for virtual devices **must** utilise separate vNICs and vLANs for standard traffic if other appropriate controls are not applied.	PR.AC-5
11.5.3	Where virtual networks span multiple physical hosts and utilise virtual switches, these **must** be distributed virtual switches where available.	PR.PT-4
11.5.4	Virtual networks **must** have some method of enabling traffic monitoring.	DE.CM-1
11.5.5	Virtual devices providing boundary functions between security domains of differing trust levels **must not** be physically co-resident with the lower trust domain and **must** comply with SS-006 Security Boundaries Security Standard [Ref. F] and SS-23 Cloud Computing Security Standard [Ref. H].	PR.DS-7

11.6 Administration of Virtualised Systems

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Administration of virtualised deployments **must** be conducted according to the principle of least privilege.	PR.AC-4
11.6.2	Restrictions and protection of administrator access to virtualisation systems **must** be in place using a virtualisation management system.	PR.AC-4

11.6.3	The remote access protocol used to access the virtualisation service **must** comply with SS-009 Hypervisor Security Standard [Ref. G].	PR.AC-3
11.6.4	Administrator account access **must** be reviewed in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. L].	PR.AC-4
11.6.5	Separate authentication solutions must be implemented for guest OSs, unless there is a specific need for two guest OSs to share credentials.	PR.AC-7

11.7 Hypervisors and Underlying Infrastructure

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Underlying hypervisors owned and managed by the Authority **must** be compliant with SS-009 Hypervisor Security Standard [Ref. G].	ID.GV-1
11.7.2	Third party or supplier managed infrastructure hosting virtual assets **must** be compliant with SS-023 Cloud Computing Security Standard [Ref. H].	ID.SC-3
11.7.3	Underlying infrastructure upon which virtualised solutions are deployed **must** be assured to the same level of security as the most secure VM that infrastructure will host.	ID.AM-5 PR.DS-5

11.8 Logging and Monitoring

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Virtualised deployments **must** be compliant with SS-012 Protective Monitoring Security Standard [Ref. I].	DE.DP-2
11.8.2	Virtual Machines **must** have a method of obtaining accurate time from the Authority Reference (Master) Clock, that takes into account the effects of virtualisation on timekeeping, in line with SS-012 Protective Monitoring Security Standard [Ref. I].	DE.DP-2
11.8.3	Virtual deployments **must** log events mandated by appropriate standards for those components (such as Server Operating System, Network Security, etc.).	DE.AE-3 DE.DP-2

11.8.4	Access to storage of Virtual Machine Images **must** be logged and monitored.	PR.PT-1
11.8.5	Administration of virtual deployments and infrastructure **must** be logged and monitored.	PR.PT-1
11.8.6	Changes to virtual deployments **must** be logged and monitored and **must** generate alerts.	PR.PT-1 DE.DP-4
11.8.7	Creation, migration, suspension or deletion of Virtual Machines **must** be logged, and safeguards **must** be in place to detect changes and generate an alert.	PR.PT-1 DE.DP-4
11.8.8	Introspection monitoring capabilities **must** include network traffic, memory, processes, and other elements of a guest OS and **must** be compliant with the SS-009 Hypervisor Security Standard [Ref. G].	DE.AE-3 DE.CM-1
11.8.9	All anomalies detected within the virtualised environment **must** be recorded.	PR.PT-1 DE.DP-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
ID.AM-2	Software platforms and applications within the organization are inventoried	11.4.1
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	11.7.3
ID.GV-1	Organizational cybersecurity policy is established and communicated	11.7.1
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.7.2
PR.AC-3	Remote access is managed	11.2.3, 11.6.3
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.5.1, 11.6.1, 11.6.2, 11.6.4
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)	11.5.2, 11.6.5
PR.DS-1	Data-at-rest is protected	11.2.2, 11.2.3, 11.3.1, 11.4.1, 11.5.4

PR.DS-5	Protections against data leaks are implemented	11.2.2, 11.7.3
PR.DS-7	The development and testing environment(s) are separate from the production environment	11.2.4
PR.IP-2	A System Development Life Cycle to manage systems is implemented	11.1.1
PR.IP-3	Configuration change control processes are in place	11.1.1
PR.IP-4	Backups of information are conducted, maintained, and tested	11.5.5
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	11.1.5
PR.IP-6	Data is destroyed according to policy	11.5.6
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.1.2
PR.IP-10	Response and recovery plans are tested	11.1.2
PR.IP-12	A vulnerability management plan is developed and implemented	11.1.3
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.2.5
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.8.4, 11.8.5, 11.8.6, 11.8.7, 11.8.9
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.8.3, 11.8.8

DE.CM-1	The network is monitored to detect potential cybersecurity events	11.8.8
DE.CM-4	Malicious code is detected	11.1.3, 11.2.1, 11.2.3
DE.DP-2	Detection activities comply with all applicable requirements	11.8.1, 11.8.2, 11.8.3
DE.DP-4	Event detection information is communicated	11.8.6, 11.8.7, 11.8.9

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-033 Security Patching Standard	Yes
B	SS-008 Server Operating System Security Standard	Yes
C	SS-007 Use of Cryptography Security Standard	Yes
D	SS-002 Public Key Infrastructure & Key Management Security Standard	Yes
E	SS-018 Network Security Design Security Standard	Yes
F	SS-006 Security Boundaries Security Standard	Yes
G	SS-009 Hypervisor Security Standard	Yes
H	SS-023 Cloud Computing Security Standard	Yes
I	SS-012 Protective Monitoring Security Standard	Yes
J	SS-035 Secure Backup and Recovery Security Standard	Yes
K	SS-036 Sanitisation and Destruction Security Standard	Yes
L	SS-001 pt.2 Privileged User Access Security Standard	Yes
M	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 800-125 Guide to Security in Full Virtualisation Technologies http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf NIST 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf
CSA Best Practices for Mitigating Risks in Virtualized Environments https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
DDA	Digital Design Authority (part of Digital Group)
NIC	Network Interface Card
pNIC	Physical Network Interface Card
vLAN	Virtual Local Area Network
VM	Virtual Machine
vNIC	Virtual Network Interface Card

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).

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