Security Standard - Virtualisation (SS-025)

Chief Security Office

Date: 20/05/2026

Department for Work & Pensions

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	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

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

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 11.1.3 Redundant VMs 11.2.1 Cloud-native/container-native services;Trusted source; added ref to SS-011 Containerisation standard 11.2.2 vendor hardening guides, configuration baselines, secure deployment practices 11.2.5 Unused VMs 11.2.6 Moved from 11.1.3; authentication bypass or access to protected data; verification; scanning 11.2.7 VMs exposed to the internet 11.3.2 Snapshot access 11.3.3 Encryption of snapshots 11.3.4 Snapshot hardening 11.3.5 Snapshot tamper-proofing 11.3.6 Snapshot lifespan and retention schedule 11.4.1 RNG and HSM; added ref to SS-002 11.4.2 Encryption key rotation; at least annually	

		11.5.5 Backup requirements 11.6.2 Isolated storage networks; Dedicated management networks 11.6.6 vNETs; over-segmentation 11.6.7 vNET controls; over-segmentation 11.7.1 limited number of admins 11.7.2 VM consoles; Lockdown Mode; Terminal Services, SSH 11.7.3 Restrict VM – Host comms 11.7.4 MFA 11.7.6 System recovery actions 11.7.7 Domain-joined hosts; on-premise vs cloud-based hypervisors 11.9.2 Authority approved time source Internal Refs – SS-011 Containerisation standard Glossary – on-premise	

3. Approval History

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

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

5. Exceptions Process

(Important) this paragraph contains 'must' activities.

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

(Important) this paragraph contains ‘must’ activities.

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 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 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

(Important) this paragraph contains ‘must’ activities.

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

(Important) this paragraph contains ‘must’ activities.

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.	ID.AM-08 PR.PS-01
11.1.2	Virtual Machines (VMs) **must** be designed to be able to gradually degrade functionality, in the case of an incident that prohibits from maintaining full functionality.	PR.IR-03
11.1.3	Services on VMs such as load balancers, DNS, Web API servers etc. **must** be removed once they are no longer needed.	PR.PS-02
11.1.4	All virtualised software, including that which is automatically provisioned, **must** be correctly and appropriately licensed.	ID.AM-02
11.1.5	Testing **must** be performed to ensure that the network infrastructure, servers, and storage can support virtualisation.	PR.IR-04

11.2 Virtual Machine Images

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	For cloud-native / container-native services, live virtualised systems **must** be created from a trusted source, containing 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. Images **must** be integrity checked and signed in line with SS-011 Containerisation security standard [Ref. N].	DE.CM-01
11.2.2	VM Images **must** be hardened in accordance with SS-008 Server Operating System Security Standard [Ref. B], as well as specific vendor hardening guides, configuration baselines, and secure deployment practices.	PR.DS-01 PR.DS-10
11.2.3	VM images **must** have controls in place to protect them from: • Malware • Unauthorised access • Unauthorised modification • Unauthorised deletion • Unauthorised copying	PR.IR-01 DE.CM-01 PR.AA-05 PR.DS-01
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-01

11.2.5	Measures **must** be in place to prevent the proliferation of images, also known as VM sprawl. Unused VMs **must** be decommissioned using regular audits and automated tooling where appropriate.	PR.PS-01 PR.PS-02
11.2.6	Virtual machines, and virtual machine images **must** be patched (or updated) in line with SS-033 Security Patching Standard [Ref. A], especially where vulnerabilities allow authentication bypass or access to protected data. Verification **must** be conducted to ensure that vulnerable services or configurations have been corrected, and checking for persistence mechanisms established prior to patching/updating. Any inactive images **must** be patched (or updated) before being put back into operation. Regular vulnerability management scanning **must** also be conducted.	PR.PS-02 DE.CM-09
11.2.7	VMs **must only** be exposed to the internet with controlled and secured exposure via appropriate boundary services.	PR.IR-01

11.3 Snapshot Management

(Important) this paragraph contains 'must' activities.

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-10

11.3.2	Access to snapshot repositories and management tools **must** be controlled in line with SS-001-1 Access & Authentication security standard [Ref. O] To ensure they aren't made unavailable through tampering.	PR.AA-05
11.3.3	Snapshots **must** be encrypted at rest and in transit in line with SS-007 Use of Cryptography security standard [Ref. C]. Encryption keys must be retained for the life of the snapshot.	PR.DS-01 PR.DS-02
11.3.4	Snapshots **must** be hardened and securely configured to ensure they are free from known vulnerabilities.	PR.PS-01 PR.PS-06
11.3.5	Snapshots **must** be made tamper-proof to prevent renaming or modification of exported snapshot images. This should be achieved by making them read-only or using methods that render the snapshot unrecoverable if illicitly renamed.	PR.DS-01 PR.PS-01
11.3.6	A creation and retention schedule for snapshots **must** be maintained and regularly audited to ensure it is being adhered to and is still relevant to the needs of the system. Maintaining too many snapshots beyond their intended lifespan could result in data that has been removed for security reasons still being available.	PR.DS-01

11.4 Encryption

(Important) this paragraph contains ‘must’ activities.

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 and can be achieved for example by using Random Number Generation (RNG), or by customer managed keys on a Authority -managed Hardware Security Module (HSM) managed in line with SS-002 PKI & Key Management security standard [Ref. D]. These capabilities may be provided at the hypervisor level.	PR.DS-01
11.4.2	Encryption keys **must** be rotated on a schedule derived from a mix of algorithm strength, key length, and the classification of information, but at least annually. Encryption keys used for snapshots **must** be retained for at least the designated lifespan of the snapshot.	PR.DS-01

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.AA-05
11.5.2	Attempts to access virtual storage solutions **must** be authenticated prior to access being granted.	PR.AA-03

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-01
11.5.4	Backups, archives, and copies of virtual storage **must** be securely stored commensurate with the security of the original source.	PR.DS-01
11.5.5	Backups of virtual drives **must** be conducted on a regular basis and **must** utilise immutable storage or air-gapped architectures to ensure recovery is possible even if the virtualised estate is compromised by ransomware. This **must** comply with the SS-035 Secure Backup and Recovery Security Standard [Ref. J].	PR.DS-11
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.DS-01

11.6 Virtual Networking

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	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.IR-01

11.6.2	Storage networks **must** be isolated, separating SAN/NAS/Fibre Channel traffic from management and production networks to limit exposure. Dedicated management networks for virtual devices **must** be utilised, with separate vNICs and vLANs for standard traffic if other appropriate controls are not applied.	PR.IR-01
11.6.3	Where virtual networks span multiple physical hosts and utilise virtual switches, these **must** be distributed virtual switches where available.	PR.IR-01
11.6.4	Virtual networks **must** have some method for enabling traffic monitoring.	DE.CM-01
11.6.5	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.IR-01
11.6.6	Virtual networks **must** be broken down into the highest number of segments as reasonable and proportionate for the services running, **must** be threat driven rather than volume, and follow approved architecture patterns (e.g. zero trust). This implements micro-segmentation, isolating workloads to reduce the lateral attack surface of any single network segment, but care **must** be taken to minimise complexity and performance impacts, as well as over-segmentation.	PR.IR-01

11.6.7	Where multiple vNETs are used, data flow between them **must** be strictly controlled. Only the explicitly required data types and connections **must** be allowed to traverse these boundaries. Care **must** be taken to not over-segment vNETS.	PR.IR-01

11.7 Administration of Virtualised Systems

(Important) this paragraph contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Administration of virtualised deployments **must** be conducted according to the principle of least privilege and limited to the smallest number of administrators possible.	PR.AA-05
11.7.2	Restrictions and protection of administrator access to virtualisation systems **must** be in place using a virtualisation management system. Hypervisors **must** be placed in Normal or Strict Lockdown Mode to ensure they can only be managed centrally, limiting and heavily auditing any exceptions. The use of VM consoles **must** be minimised in favour of Terminal Services and SSH; however, host-level SSH and local shells **must** be disabled by default and only enabled temporarily for troubleshooting.	PR.AA-05
11.7.3	The remote access protocol used to access the virtualisation service **must** comply with SS-009 Hypervisor Security Standard [Ref. G]. Communications between VMs and hosts **must** be restricted to reduce the risk of a compromised VM spreading malware to the host or to other VMs.	PR.DS-02

11.7.4	Administrator account access **must** require Multi Factor Authentication in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. L].	PR.AA-05
11.7.5	Separate authentication solutions **must** be implemented for guest OSs, unless there is a specific need for two guest OSs to share credentials.	PR.AA-03
11.7.6	Systems **must** be designed to recover into a secure state, ensuring all encryption and access controls are fully applied following unplanned shutdowns or power drops. Automated recovery sequences should be utilised where safe, balancing rapid availability against the risk of booting into a vulnerable state. Recovery actions are not complete until this secure state has been verified.	RC.RP-04 RC.RP-05
11.7.7	For on-premise hosted hypervisors, hosts **must** not be joined to standard enterprise Active Directory (AD) domains. Domain-joined hosts increase lateral movement risk and expose the infrastructure to AD-based privilege escalation (e.g. ticket forgery or exploitation of default admin groups). Administration **must** instead rely on strong local credentials, identity federation or physically and logically separate identity stores. This requirement does not apply to cloud-based hypervisors, where the Authority does not control the hypervisor.	PR.AA-01 PR.IR-01

11.8 Hypervisors and Underlying Infrastructure

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Underlying hypervisors owned and managed by the Authority **must** be compliant with SS-009 Hypervisor Security Standard [Ref. G].	PR.PS-01
11.8.2	Third party or supplier managed infrastructure hosting virtual assets **must** be compliant with SS-023 Cloud Computing Security Standard [Ref. H].	GV.SC-05
11.8.3	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.	PR.DS-01 PR.DS-10

11.9 Logging and Monitoring

(Important) this paragraph contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Virtualised deployments **must** be compliant with SS-012 Protective Monitoring Security Standard [Ref. I].	DE.CM-01 DE.CM-09
11.9.2	Virtual Machines **must** have a method of obtaining accurate time from an Authority approved time source, that takes into account the effects of virtualisation on timekeeping, in line with SS-012 Protective Monitoring Security Standard [Ref. I].	PR.IR-01

11.9.3	Virtual deployments **must** log events mandated by appropriate standards for those components (such as Server Operating System, Network Security, etc.).	PR.PS-04
11.9.4	Access to storage of Virtual Machine Images **must** be logged and monitored.	PR.PS-04 DE.CM-03
11.9.5	Administration of virtual deployments and infrastructure **must** be logged and monitored.	PR.PS-04
11.9.6	Changes to virtual deployments **must** be logged and monitored and **must** generate alerts.	PR.PS-04
11.9.7	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.PS-04
11.9.8	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.CM-01 DE.CM-09
11.9.9	All anomalies detected within the virtualised environment **must** be recorded.	PR.PS-04 DE.CM-09

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
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritised, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	11.8.2
ID.AM-02	Inventories of software, services, and systems managed by the organisation are maintained	11.1.4
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.1
PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.7.7
PR.AA-03	Users, services, and hardware are authenticated	11.5.2, 11.7.5

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	11.2.3, 11.3.2, 11.5.1, 11.7.1, 11.7.2, 11.7.4
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.2.2, 11.2.3, 11.2.4, 11.3.3, 11.3.5, 11.3.6, 11.4.1, 11.4.2, 11.5.3, 11.5.4, 11.5.6, 11.8.3
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.3.3, 11.7.3
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.2.2, 11.3.1, 11.8.3
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.5.5
PR.PS-01	Configuration management practices are established and applied	11.1.1, 11.2.5, 11.3.4, 11.3.5, 11.8.1
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.3, 11.2.5, 11.2.6
PR.PS-04	Log records are generated and made available for continuous monitoring	11.9.3, 11.9.4, 11.9.5, 11.9.6, 11.9.7, 11.9.9
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	11.3.4
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.2.3, 11.2.7, 11.6.1, 11.6.2, 11.6.3, 11.6.5, 11.6.6, 11.6.7, 11.7.7, 11.9.2

PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	11.1.2
PR.IR-04	Adequate resource capacity to ensure availability is maintained	11.1.5
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.2.1, 11.2.3, 11.6.4, 11.9.1, 11.9.8
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.9.4
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.2.6, 11.9.1, 11.9.8, 11.9.9
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	11.7.6
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	11.7.6

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
N	SS-011 Containerisation security standard	Yes
O	SS-001-1 Access & Authentication security standard	Yes

*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).
On-premise	Locally installed software that runs on an organisation's own IT environment

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