IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard – Virtualisation (SS-025)

Chief Security Office

Date: 17/07/2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

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

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

1. Introduction

1.1. This Virtualisation Security Standard provides the list of controls that are required to secure virtualised deployments to a Department for Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data to be stored or handled by virtualised systems. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for virtualisation and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for virtualised deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

3. Exceptions

3.1. In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to Design Authority (DA) where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

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

3.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for suppliers to, and members of, DWP Infrastructure and Operational Services (IOS), who are involved in building, procuring, and/or securing virtualised environments for DWP systems and applications.

5. Scope

5.1. This standard is applicable to all deployments upon virtualised infrastructure, where there is hardware virtualisation. This includes virtual machines, virtual storage, and virtual networks.

5.2. This standard does not cover:

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

5.3. This standard is applicable to systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP), including that with the OFFICIAL-SENSITIVE handling caveat. All of the organisation's virtualised deployments falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.4. The security control requirements laid out in this standard are product agnostic and applicable for all virtualised deployments that are provisioned for departmental use.

5.5. In the event of uncertainty on the controls laid out in this standard please contact the Security Front Door for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

7.1. Governance

Reference	Security Control Requirement
7.1.1.	An asset register of all virtual assets MUST be maintained and updated as appropriate. This includes recording: • VM creation • VM destruction • VM modification • Owners for those assets
7.1.2.	There MUST be controls in place to prevent unauthorised creation, destruction, or copying of virtual machines
7.1.3.	Virtual Machines MUST have disaster recovery and business continuity controls.
7.1.4.	Virtual machines, and virtual machine images, including those not currently active, MUST be patched in line with DWP patching policy.
7.1.5.	Virtual assets MUST be subject to an appropriate change management process.
7.1.6.	All virtualised software, including that which is automatically provisioned, MUST be correctly and appropriately licensed.

7.2. Virtual Machine Images

Reference	Security Control Requirement
7.2.1.	Live virtualised systems MUST be created from pre-configured, system images (VM Images)
7.2.2.	VM Images MUST be hardened in accordance with Security Standard – Server Operating System
7.2.3.	VM images MUST have controls in place to protect them from: • Malware • Unauthorised access • Unauthorised modification • Unauthorised deletion • Unauthorised copying
7.2.4.	VM Images MUST be stored in a storage location logically separate from the storage location where inactive or dormant VMs are stored.
7.2.5.	VM images MUST be patched or kept up to date in the same manner as live systems.

7.3. Encryption

Reference	Security Control Requirement
7.3.1.	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.
7.3.2.	Persistent encryption keys MUST be generated on physical machines only and securely transferred to virtual machines, in line with Security Standard – Use of Cryptography.
7.3.3.	Encryption Keys MUST be protected and backed up in accordance with Security Standard – Public Key Infrastructure

7.4. Virtual Storage

Reference	Security Control Requirement
7.4.1.	Access to virtual storage solutions MUST be restricted only to users and functions that require access to that storage.
7.4.2.	Attempts to access virtual storage solutions MUST be authenticated prior to access being granted.
7.4.3.	Encryption of virtual storage MUST be in accordance with Security Standard – Use of Cryptography
7.4.4.	Backups, archives, and copies of virtual storage MUST be stored with commensurate security to the original source.
7.4.5.	Virtual storage MUST be securely sanitised before being re-allocated or decommissioned.

7.5. Virtual Networking

Reference	Security Control Requirement
7.5.1.	Standard network controls MUST be applied to virtualised networks as if they were physical networks, in compliance with Security Standard – Network Security Design.
7.5.2.	Management networks for virtual devices MUST utilise separate vNICs and vLANs to standard traffic.
7.5.3.	Where virtual networks span multiple physical hosts and utilise virtual switches, these MUST be distributed virtual switches where available.
7.5.4.	Virtual Appliances MUST be virtualisation aware.
7.5.5.	Virtual networks MUST have some method of enabling traffic monitoring.
7.5.6.	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 Security Standard – Security Boundaries.

7.6. Administration

Reference	Security Control Requirement
7.6.1.	Administration of virtualised deployments MUST be conducted according to the principle of least privilege.

7.7. Hypervisors and Underlying Infrastructure

Reference	Security Control Requirement
7.7.1.	Underlying hypervisors owned and managed by DWP MUST be compliant with Security Standard – Hypervisor.
7.7.2.	Third party or supplier managed infrastructure hosting virtual assets MUST be compliant with SS-023 Security Standard – Cloud Computing.
7.7.3.	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.

7.8. Logging

Reference	Security Control Requirement
7.8.1.	Virtualised deployments MUST be compliant with Security Standard – Protective Monitoring.
7.8.2.	Virtual Machines MUST have a method of obtaining accurate time that takes into account the effects of virtualisation on timekeeping, in line with Security Standard – Protective Monitoring.
7.8.3.	Virtual deployments MUST log events mandated by appropriate standards for those components (such as Server Operating System, Network Security, etc.).
7.8.4.	Access to storage of Virtual Machine Images must be logged.
7.8.5.	Administration of virtual deployments and infrastructure MUST be logged.
7.8.6.	Changes to virtual deployments MUST be logged and MUST generate alerts.
7.8.7.	Creation, migration, suspension or deletion of Virtual Machines MUST be logged and MUST generate an alert.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 24 months of the approval of the standard.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		
DWP Baseline Control Set		
Standard Master List		
DWP Patching Policy		

11. Reference Documents

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

12. Definition of Terms

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).

13. Glossary

Abbreviation	Definition
DA	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

14. Controls Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP Application Security Verification Standard (ASVS.

SS-024 Virtualisation Control Statement	DWP Controls Catalogue - Baseline Control Set	
	Control Reference	Descriptor
10.1.1	AS01	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
	AS02	Assets maintained in the inventory shall be owned.
10.1.2	-	
10.1.3	BC02	The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
	BC05	Back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
10.1.4	-	
10.1.5	GV01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.
10.1.6	LG01	Installing commercially licensed software in a cloud service can cause a breach of the licence terms for the software. The cloud service customer should have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and the software can be run on more systems or processor cores than is permitted by the licence terms.
10.2.1	CLC03	When configuring virtual machines, cloud service customers and cloud service

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-024 Virtualisation Control Statement	DWP Controls Catalogue - Baseline Control Set	
	Control Reference	Descriptor
		providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.
10.2.2	CLC03	When configuring virtual machines, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.
10.2.3	MW01	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
	MW03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
10.2.4	-	
10.2.5	-	
10.3.1	-	
10.3.2	-	
10.3.3	-	
10.4.1	-	
10.4.2	-	
10.4.3	-	
10.4.4	-	
10.4.5	PH13	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
	MH02	Media shall be disposed of securely when no longer required, using formal procedures to ensure data cannot be recovered.
10.5.1	CSP07	The cloud service provider should define and document an information security policy for the configuration of the virtual network consistent with the information security policy for the physical network. The cloud service provider should ensure that the virtual network configuration matches the information security policy regardless of the means used to create the configuration.
	NT02	Network environments and virtual instances shall be designed and configured to restrict

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-024 Virtualisation Control Statement	DWP Controls Catalogue - Baseline Control Set	
	Control Reference	Descriptor
		and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.
	NT03	Networks shall be managed and controlled to protect information in systems and applications.
10.5.2	-	
10.5.3	-	
10.5.4	-	
10.5.5	-	
10.5.6	-	
10.6.1	-	
10.7.1	-	
10.7.2	-	
10.7.3	-	
10.8.1	-	
10.8.2	EV07	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source. A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.
10.8.3	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
10.8.4	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
10.8.5	EV05	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
10.8.6	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
	EV05	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
10.8.7	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
	EV05	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.