Security Standard – Hypervisor (SS-009)

Chief Security Office

Date: September 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 Hypervisor Security Standard provides the list of controls that are required to secure Hypervisor implementations 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 in these implementations. 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 Hypervisors 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 Hypervisor deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits and IT Health Checks (ITHCs).

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 the DWP Design Authority (DA) advisory or governance board, 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 the application’s risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for consumption by suppliers, technical architects, database administrators, developers, security groups, and also IT staff such as security compliance teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL and OFFICIAL-SENSITIVE tier of the Government Security Classification Policy (GSCP). All of the organisation's Hypervisor implementations; both type 1 and type 2, 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.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all Hypervisor systems that are provisioned for departmental use which can be accessed and altered by the Department.

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 to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

7.1. Hypervisor Platform Architectural Choices

Reference	Security Control Requirement
7.1.1.	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.
7.1.2.	There MUST be consideration of the platform virtualisation approach that would be most suitable for the Department's need. A Hypervisor platform with hardware assisted virtualisation (both instruction set and memory management) provides greater security assurance than one with purely software assisted virtualisation because of the following: • Better memory management controls can prevent attacks such as buffer overflow. • Better protection for device access mediation functions through privilege level isolation and better VM-level protection through hardware-based memory protection. • By supporting full virtualisation, COTS versions of O/Ss can be run enabling easier patching/updating than having to perform the same operations on modified/ported versions of O/Ss that are the only types that can be run on para virtualised platforms. • Since many features of virtualisation are now available in hardware, the size of the hypervisor code will be small enabling better security attestation/verification.
7.1.3.	The hypervisor that is launched MUST be part of a platform and an overall infrastructure that contains: (a) Hardware that supports a Measured Launch Environment (MLE) and standards-based Trusted Platform Module (TPM) and (b) Attestation process that MUST contain capabilities to take advantage of these so as to provide a chain of trust starting from the Hardware to all Hypervisor components. The chain of trust provides assurance that all launched components (starting from BIOS,

Reference	Security Control Requirement
	hypervisor and device drivers) have not been tampered with and that their versions are correct (i.e., overall boot integrity).
7.1.4.	A functional Hypervisor management console with smaller code and disk footprint and smaller number of exposed interfaces can provide better security assurance by facilitating easier verification and presenting a smaller attack surface.

7.2. Device Emulation & Access Control

Reference	Security Control Requirement
7.2.1.	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.
7.2.2.	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).
7.2.3.	The access control solution for VM administration MUST have the ability to specify 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.
7.2.4.	The number of user accounts (including privileged accounts) requiring direct access to hypervisor host MUST be limited to only those that are absolutely necessary.
7.2.5.	Access to the hypervisor MUST be restricted according to least privilege and need to know basis.

7.3. VM Management

Reference	Security Control Requirement
7.3.1.	The ratio of the combined configured memory of all VMs to the RAM memory of the virtualised host MUST be no greater than 1.5:1. e.g. If a virtualised host has 64GB of RAM, then the combined configured memory of all VMs running on it MUST not exceed 96GB.
7.3.2.	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.
7.3.3.	The number of virtual CPUs allocated to any VM deployed MUST be strictly less than the total number of cores in the hypervisor host.
7.3.4.	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.
7.3.5.	There MUST be a mechanism for security monitoring and security policy enforcement of VM operations – malicious processes running inside VMs and malicious traffc going in and out of VM. This monitoring and enforcement mechanism forms the foundation for building Anti-Virus (AV) and Intrusion Detection & Prevention (IDPS) solutions.
7.3.6.	Solutions for Security Monitoring and security policy enforcement of VMs MUST be compliant with Security Standard – Virtualisation.

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.

7.4. Administration of Hypervisor Host & Hypervisor Software

Reference	Security Control Requirement
7.4.1.	If possible, the user accounts (including privileged accounts) on the hypervisor host MUST be integrated with the enterprise directory infrastructure in order to enable authentication through robust authentication protocols (e.g., Kerberos), enable enforcement of some corporate security policies (e.g., password policies) as well as handle changes to user account list (addition and deletion of user accounts).
7.4.2.	The use of administrative functions MUST be restricted to defined endpoint networks and devices, such as specific laptops or desktops that have been approved for such access.
7.4.3.	Multi-factor authentication MUST be required for all administrative functions.
7.4.4.	Administrative functions MUST be separate such that hypervisor admistrators do not have the ability to modify, delete, or disable hypervisor audit logs.
7.4.5.	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.
7.4.6.	The remote access protocol used to access the hypervisor service console MUST have configuration options available to: completely deny access (i.e., disable remote acess via specific protocols), deny hypervisor root account access and restrict access only to a specified list of administrative accounts.
7.4.7.	Use Hypervisor features that enable: • Definition of a complete set of configuration settings (Gold Configuration) for a hypervisor deployment • Automate application of those configuration settings to a new or existing hypervisor installation and, • Check compliance of existing hypervisor installation against those configuration settings, if available, in order to minimise manual configuration errors that may increase the security risk.
7.4.8.	You MUST patch the Hypervisor host and software with the most recent, secure, satisfactorily tested code at least every six months.
7.4.9.	The built-in firewall for the hypervisor MUST only be configured to allow ports and protcols (network traffic) needed for enabled services in the hypervisor, such as management and specialised security agents and third-party applications.
7.4.10.	The hypervisor MUST have a logging feature that generates logs in a standardised format (e.g., syslog as opposed to a proprietary format) to help leverage the use of tools with good analytical capabilities.
7.4.11.	The configuration of 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.
7.4.12.	The Protection of VM Management and Hypervisor Host & Software administration functions MUST be ensured by placing the management interface of the hypervisor in a dedicated virtual network segment and enforcing traffic controls using a firewall (e.g., designating the subnets in the enterprise network from which incoming traffic into the management interface is allowed).
7.4.13.	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.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	At the next IT Health Check

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	TBD	N/A
DWP Baseline Control Set		
Standard Master List		N/A

11. Reference Documents

DWP Digital Blueprint

Csrc.nist.gov. (2014) *Security Recommendations for Hypervisor Deployment* [online] October 2014. Available from: http://csrc.nist.gov/publications/drafts/800-125a/sp800-125a_draft.pdf [Accessed: 13th April 2017]

Pcisecuritystandards.org (2011) PCI DSS Virtualization guidelines [online] June 2011. Available from: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf [Accessed: 6th June 2017]

12. Definition of Terms

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.

Term	Definition
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.

13. Glossary

Abbreviation	Definition
AV	Anti-Virus
BIOS	Basic input/output system
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
DA	Design Authority
DWP	Department for Work and Pensions
IDPS	Intrusion Detection & Prevention System
MLE	Measured Launch Environment
O/S	Operating System
QEMU	Quick Emulator
RAM	Random-access memory
SVA	Security Virtual Appliance
TPM	Trusted Platform Module
VM	Virtual Machine

14. Controls Catalogue Mapping

The requirements in this document are derived from the high-level controls prescribed in the DWP Controls Catalogue