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 – Containerisation (SS-011)

Chief Security Office

Date: September 2017

Department for Work & Pensions

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.

Contents

1. Introduction

1.1. This Containerisation Security Standard provides a list of controls to help secure solutions using this technology 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. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.2. This document seeks to present non product specific security best practices and security control requirements.

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

1.4. Furthermore the security controls presented in this standard are taken from examples of international best practice for containerisation and have been tailored for Departmental suitability.

2. Purpose

2.1. This standard lists security requirements on how to deploy, implement and control the usage of Containerisation technology.

2.2. Projects should consume this documentation to ensure that the best practices for their system are being adequately and accurately addressed.

3. Exceptions

3.1. 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 DA where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.2. 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.

4. Audience

4.1. This standard is intended for suppliers, system administrators, security groups, and IT staff involved in securing environments for DWP systems and applications and gives requirements on how to manage, implement and configure containerisation technology.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP).

5.2. Implementations of containerisation MUST meet all the requirements in this standard or gain authorisation with DWP security architectural risk review (see exemptions process).

5.3. In the 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 penetration test to provide evidence of adequacy and effectiveness.

7. Overview of Application Containerisation.

NIST draft standard 800-190 Application Container Security Guide contains the following description of Application Containers.

“Application container technologies, also known as containers, are a form of operating system virtualization combined with application software packaging. Containers provide a portable, reusable, and automatable way to package and run applications.”

Application Containerisation is a mechanism to allow applications to run on a single host operating system, but with a degree of isolation from each other. With traditional Hyper Visor approaches to virtualisation, a virtual machine image would contain the “Virtual Hardware” configuration and a full copy of the operating system environment. In contrast containers are reliant on the host operating system for basic resources and services.
Therefore the degree of isolation is less than that provided by an assured Hypervisor. Containers operate using the concept of a Runtime environment; it is this layer that abstracts the underlying operating system of the host from the containers and provides the isolation between the containers executing on the host.

Containerisation supports the DevOps development and deployment models as it allows containers to be built that contain the complete service package. This allows faster deployment than traditional methods. The package will contain both business logic and supporting components.

This means that the Hosts themselves should not need configuration changes in order to receive an application. All the host will need to provide is the Container Runtime environment. This model will allow the shipping and running of any software application in a lightweight isolated computation unit.

Containerisation together with the use of Microservices allows functional components of an application to be modified, whilst having a constrained and limited impact on other components.

Containerisation technologies are available for both Linux and Windows platforms details of particular implementation guidance to meet this standard will be captured within the patterns for the specific technology.

8. Technical Security Control Requirements

8.1 Platform Hardening

Reference	Security Control Requirement
8.1.1.	The Underlying operating system supporting the containers MUST be hardened in accordance with the DWP server build standards and patterns. In addition, where specific guidance and recommendations relating to the secure use of Containerisation on the platform are available this guidance MUST be followed.
8.1.2.	Containers MUST not be used to separate data or services that have different security profiles or different Security Classifications. All containers within a single host must share the same security characteristics.
8.1.3.	Hosts MUST be set up such that, by default, network stacks within the containers on the host cannot inter-communicate. When containers are run, they MUST obtain their own individual network stack.
8.1.4.	Container Resources and kernel calls MUST be restricted to prevent Denial of Service (DOS) attacks form successful compromises of the container and potentially compromise other containers on the server.
8.1.5.	Systems administrations MUST whitelist rather than blacklist those container capabilities not required. Explicitly allow only what is needed.

8.2. Container Process Attack Surface

Reference	Security Control Requirement
8.2.1.	Privilege access management MUST be configured so that only trusted users and Application Programming Interface (API's) are able to control the Containerisation process.
8.2.2.	Secrets and credentials such as username, passwords, and keys MUST be protected and MUST not be persistent within the image.
8.2.3.	Privilege access management MUST be configured so that access to the Container control API is available only to trusted users.
8.2.4.	The container MUST externally present only the necessary ports and services required by the consuming business or administrative services.

8.3. Best Practices

Reference	Security Control Requirement
8.3.1.	Identification of all images and versions MUST be maintained at all times in the DWP's CMDB.
8.3.2.	Patching of container images must be maintained as per the DWP's policies.
8.3.3.	The patching and update process must ensure that both the offline (stored) image and runtime image are updated.
8.3.4.	Containers must meet the DWP's protective monitoring requirements as defined within the Protective Monitoring Standard.
8.3.5.	When critical vulnerabilities to the container environment are disclosed updates must be applied within 24 hours.
8.3.6.	Updates must be maintained to n-1 of latest releases unless a critical release deems a shorter time frame.
8.3.7.	On Linux implementations The administrator must disable the 'setuid' and 'setgid' binaries if they are not specifically used by applications. This will limit privilege escalation attacks.
8.3.8.	Change management process applied to containers MUST include the use of tools to examine the security configuration of the container environment and any identified weaknesses remediated.
8.3.9.	Systems Administrators MUST only use approved official Container images as a source when building DWP images, and MUST be responsible for keeping them updated regularly.

8.4. Container Configuration Policies

Reference	Security Control Requirement
8.4.1.	System Administrators MUST ensure that remote terminal access into the container is disabled.
8.4.2.	All logs MUST be managed by a process executing outside the Container and MUST NOT be managed by a process running inside the container.
8.4.3.	As part of the container configuration, commands and capabilities not required to support the service provided by the container MUST be removed or disabled.
8.4.4.	Network specific operations MUST be disabled inside containers. Network configuration MUST be applied to the container at startup and not be dynamically modified.
8.4.5.	Mount operations MUST NOT be allowed within the container.
8.4.6.	In order to mitigate malicious network activity related to packet spoofing, access to raw sockets MUST NOT be allowed within the container.
8.4.7.	Run File systems in containers MUST be read only in order to prevent malicious scripts being saved or files being overwritten.
8.4.8.	Containers MUST not be allowed to load Modules dynamically. All code that is required to execute within the container must be within the container image.

Reference	Security Control Requirement
8.4.9.	During the build process, System Administrators MUST verify and authenticate the identity of all dependencies using code signing and signatures.
8.4.10.	Systems Administrators MUST enforce the use of the most up to date image dependencies.
8.4.11.	When container images are saved to a repository they MUST be validated and signed before being stored.
8.4.12.	System Administrators MUST add a signature at each stage of the build and deploy process to ensure the integrity of the container Image before it is promoted through the environments...
8.4.13.	All diagnostics in production MUST be done via log files.
8.4.14.	System Administrators MUST ensure that where the Container environment distribution ships with security model templates, Containers are built using the appropriate template.

8.5. Container Best Practices

Reference	Security Control Requirement
8.5.1.	Each container and process MUST run with the minimum set of resources and access rights it requires to perform its intended function
8.5.2.	System Administrators MUST ensure only a single instance, of a single application or Microservice is run per container. Processes MUST not be daemonised within single containers and multiple applications MUST not be run in single containers.
8.5.3.	System Administrators MUST not treat containers as Virtual Machines. If the application has multiple components that need to run distinctly from one another, then run each component in its own container.
8.5.4.	Services between containers MUST be exposed only via port binding, with ports explicitly opened in a Container configuration file, specifying that the only permitted connection to a given application is from another container.
8.5.5.	Each application SHOULD ideally only be bound to one port, and this must also be reflected in the container configuration. This ensures that a container only exposes a single port, discretely representing the service it is running.
8.5.6.	Orchestration tools for managing the Build, Distribution and Run phases of the Container Lifecycle MUST be used supported by a CMDB

9. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

10. 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.

11. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		

12. Reference Documents

DWP Digital Blueprint

13. Definition of Terms

Term	Definition
Containers	A running instance of an image
Image	The executable result of building a container

14. Glossary

Abbreviation	Definition
API	Application Programming Interface
DevOps	Development and Operations
ISO	International Organization for Standardization

15. Controls Catalogue 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 ASVS. NIST have published a draft standard for containers under the 800 series of publications 800- 190 “Application Container Security Guide”.

SS26 Containerisation	**DWP Controls Catalogue - Baseline Control Set**	
10.1.1	OP01	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
10.1.2	NT01	Separation of development, test and operational environments
10.1.3	NT02	Infrastructure & Virtualization Security Network Security
10.1.5	OP01	As 11.1.1
10.2.1	AC02, AC08, AC21	Access to networks and network services, Management of privileged, Use of privileged utility programs access rights,
10.2.2	AC11	Management of secret authentication information for users
10.2.3	AC02, AC08, AC21	As 12.1.1
10.2.4	OP1	As 11.1.1
10.3.1	AS01	Inventory of assets
10.3.2	AP07	Threat and Vulnerability Management Vulnerability / Patch Management
10.3.3	AP07	As 13.1.2
10.3.4	EV04,EV05,EV07	Protection of log information, Administrator and operator logs, Clock synchronisation
10.3.5	AP07	As 13.1.2
10.3.6	AP07	As 13.1.2
10.3.7	AC08	Management of privileged access rights
10.3.8	AP07	As 13.1.2
10.3.9	AS01	Inventory of assets
10.4.1	OP01	As 11.1.1
10.4.2	OP01	As 11.1.1
10.4.3	OP01	As 11.1.1
10.4.4	OP01	As 11.1.1
10.4.5	OP01	As 11.1.1
10.4.6	OP01	As 11.1.1
10.4.7	OP01	As 11.1.1
10.4.8	OP01	As 11.1.1

SS26 Containerisation	**DWP Controls Catalogue - Baseline Control Set**	
10.4.9	OP01	As 11.1.1
10.4.10	AS01	Inventory of assets
10.4.11	AS01	Inventory of assets
10.4.12	OP01	As 11.1.1
10.4.14	OP01	As 11.1.1
10.5.1	OP01	As 11.1.1
10.5.2	OP01	As 11.1.1
10.5.3	OP01	As 11.1.1
10.5.4	OP01	As 11.1.1
10.5.5	OP01	As 11.1.1
10.5.6	OP01	As 11.1.1