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 – Server Operating System (SS-008)

Chief Security Office

Date: 26/05/2017

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

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.

1. Introduction

1.1. This Security Standard provides a list of security controls that apply to all server deployments. This list of requirements ensures a baseline level of security that is approved and accepted by the Department for Work and Pensions (DWP) to afford the necessary level of protection to its systems and data.

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 examples of international best practice for server security 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 secure server 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.

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.

4. Audience

4.1. This standard is intended for (but not limited to) security controls testing consultants, solution, domain and security architects and system designers as well as engineers and/or system administrators who are provisioning servers for departmental use.

5. Scope

5.1. The security controls presented in this document are applicable to any server deployments within the DWP. This includes specialist server operating systems (such as Windows Server 2016) as well as generic or desktop operating systems upon which server applications will be, or are, installed.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all operating systems that are provisioned for departmental use as servers.

5.3. Additional controls may be applicable based upon the server application that is ultimately installed upon the operating system.

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. Operating System Selection

Reference	Security Control Requirement
7.1.1.	Server operating systems MUST be of a version that is still under active vendor support. This must include security patches for identified vulnerabilities with a CVE score of 7 or greater.
7.1.2.	Server operating systems MUST utilise a version that complies with DWP software version policy.
7.1.3.	Servers that will store or handle citizen data MUST utilise an operating system that is certified to a minimum of EAL4 or successor standards.

7.2. Installation

Reference	Security Control Requirement
7.2.1.	Server operating systems MUST only be installed from a trusted source.
7.2.2.	Server operating systems MUST only be connected to trusted networks during the install process.

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.

Reference	Security Control Requirement
7.2.3.	Server operating system installations MUST include all current approved service packs / major releases for that operating system version.
7.2.4.	Server operating system installations MUST apply all approved and verified updates and patches not already included on installation media immediately subsequent to installation.
7.2.5.	Where configuration changes are required to maintain EAL4 certification (or equivalent) to comply with 10.1.3 above, these MUST be applied immediately subsequent to installation.

7.3. General Configuration

Reference	Security Control Requirement
7.3.1.	Server operating systems MUST utilise an approved secure file system (such as NTFS or EXT4).
7.3.2.	Server operating systems MUST be configured to receive accurate time from an appropriate time source, in compliance with Security Standard - Protective Monitoring.
7.3.3.	Server operating systems that upload telemetry and personalisation data to third parties MUST have controls in place or be configured to, prevent this where such upload is not necessary.
7.3.4.	Any operating system controls to protect system and application memory MUST be enabled.
7.3.5.	Server operating systems MUST be configured so they do not auto-run inserted media.
7.3.6.	Server operating systems MUST be patched in line with DWP patching policy.
7.3.7.	Servers with Network Interface Cards (NIC's) connecting to domains of differing trust levels MUST prevent traffic being bridged between those domains, except where the server is performing security functions for this explicit purpose (see Security Standard – Security Boundaries).
7.3.8.	Servers MUST utilise separate NIC's for differing traffic types, in accordance with the Security Standard -Secure Network Design.

7.4. Applications and Services

Reference	Security Control Requirement
7.4.1.	All unnecessary applications and features on servers MUST be disabled, and removed where possible.
7.4.2.	There MUST be measures in place to prevent installation of unauthorised applications or features onto servers.
7.4.3.	Servers MUST be limited to performing one function only (such as web server, email server, file server, etc.).
7.4.4.	All operating system services not essential to the role and function of the server MUST be disabled.
7.4.5.	All servers MUST have an anti-malware solution installed and operating, in line with the Security Standard - Malware Protection.

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.

Reference	Security Control Requirement
7.4.6.	Server applications MUST have their access to system resources limited to the minimum required to operate correctly.
7.4.7.	Applications or services capable of circumventing or changing system controls MUST have their access restricted.

7.5. Firewalls

Reference	Security Control Requirement
7.5.1.	Server deployments MUST have a suitable host-based firewall configured and turned on (such as Windows Firewall, IPtables, etc.).
7.5.2.	Servers MUST be deployed in a suitably protected location as defined by Security Standard – Network Security Design.
7.5.3.	Server firewalls MUST be set up to block all traffic by default, and only allow explicitly defined traffic.
7.5.4.	Server firewalls MUST be configured to allow inbound or outbound traffic only on ports that are necessary to the operation of the system.
7.5.5.	Servers MUST have any internet browser applications (such as Internet Explorer) removed or disabled.

7.6. Administration

Reference	Security Control Requirement
7.6.1.	Server accounts MUST restrict administrative actions and access via Role-Based Access Control (RBAC) (such as through use of UAC or sudo).
7.6.2.	Remote administration MUST be conducted through approved secure channels (such as SSH, IPsec VPN, etc.).
7.6.3.	Remote administration of servers MUST be carried out in accordance with the Security Standard - Remote Access.
7.6.4.	All default passwords on all accounts MUST be changed, and comply with the Security Standard - Password Management.
7.6.5.	Administration of servers MUST be carried out from dedicated management infrastructure.

7.7. User Accounts

Reference	Security Control Requirement
7.7.1.	All server user accounts MUST be provisioned in accordance with the principle of least privilege.
7.7.2.	All server user accounts MUST enable individual users to be identified (e.g. unique accounts per user, or logged access to shared accounts).
7.7.3.	Guest accounts MUST be removed.
7.7.4.	Servers MUST implement measures to limit or prevent exposure of account names.
7.7.5.	All servers MUST implement some form of account or session lock after no more than 10 failed login attempts. The form this takes

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.

Reference	Security Control Requirement
	(hard/soft lockout, time period, unlock procedures) MUST be determined in a risk-based manner, taking into account system function, data handled, and account privileges.
7.7.6.	User accounts on servers MUST be removed when they are no longer required.
7.7.7.	User accounts on servers MUST be reviewed at least every 6 months and be removed if they are no longer required.
7.7.8.	User accounts on servers MUST be evaluated at least every six months to ensure the permissions assigned to them are still appropriate.
7.7.9.	Revoked or disabled accounts MUST only be re-issued to the individual that the account is currently assigned to.
7.7.10.	User accounts MUST automatically terminate user sessions (either by logging off or locking) after being inactive for no more than 10 minutes.

7.8. Service Accounts

Reference	Security Control Requirement
7.8.1.	All server service accounts MUST be provisioned in accordance with the principle of least privilege.
7.8.2.	Service accounts MUST be unique accounts that are not shared with human users.
7.8.3.	Service accounts MUST limit the number of services that access them.
7.8.4.	Service accounts MUST have interactive login disabled.
7.8.5.	Service accounts on servers MUST be removed when they are no longer required.
7.8.6.	Service accounts on servers MUST be reviewed at least every six months, and be removed if they are no longer required.

7.9. Authentication Credentials

Reference	Security Control Requirement
7.9.1.	All passwords used on servers MUST be compliant with the requirements of the Security Standard - Password Management Access Control.
7.9.2.	Credentials MUST be stored and protected in line with Security Standard - Use of Cryptography.
7.9.3.	Credentials for operating system accounts MUST be unique per account.
7.9.4.	Server operating systems MUST have technical controls implemented to ensure passwords assigned to human users have appropriate lifetimes, in compliance with DWP password policy.

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.

7.10. Physical Access Control

Reference	Security Control Requirement
7.10.1.	Physical access to hardware hosting any server operating system MUST be restricted appropriately in accordance with the Physical Access Policy.

7.11. Logical Access Control

Reference	Security Control Requirement
7.11.1.	Servers MUST be compliant with the Security Standard – Secure Access and Authentication.
7.11.2.	Servers MUST ensure access to system resources is authorised appropriately.
7.11.3.	Servers MUST require credentials when waking from sleep, hibernation, or suspended operation.
7.11.4.	Servers MUST prevent remote access to Plug and Play (PNP) services.

7.12. Backup

Reference	Security Control Requirement
7.12.1.	Servers MUST be backed up in accordance with the Secure Backup Standard.
7.12.2.	Server backups MUST prevent access to application data without the appropriate cryptographic keys.

7.13. System Logging

Reference	Security Control Requirement
7.13.1.	All logging carried out on servers MUST be conducted in accordance with the Security Standard - Protective Monitoring.
7.13.2.	All logs produced on servers MUST be forwarded to the appropriate centralised log collection point, in compliance with the Security Standard – Protective Monitoring.
7.13.3.	All attempts to change server configurations MUST be logged.
7.13.4.	Any events which involve privilege escalation MUST be logged.
7.13.5.	Log on / log off events MUST be logged.
7.13.6.	Actions that modify or create users or groups, or modify the privileges of users or groups on servers, MUST be logged.
7.13.7.	Shutdown and system suspension events on servers MUST be logged.
7.13.8.	Failed object access or privilege use MUST be logged.

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.

7.14. Monitoring and Alerting

Reference	Security Control Requirement
7.14.1.	Alerts MUST be generated in accordance with the Security Standard – Protective Monitoring
7.14.2.	Processes invoked in response to alerts MUST be compliant with Security Standard – Incident Management
7.14.3.	Alerts MUST be generated for any events that would prevent core server functionality
7.14.4.	Alerts MUST be generated for any event or combination of events that is indicative of unusual user or process activity.
7.14.5.	Failed authentication events MUST generate an alert.

7.15. Directory Servers

Reference	Security Control Requirement
7.15.1.	Any servers providing directory functions (such as Domain controllers, LDAP, RADIUS etc.) MUST only be created from fresh operating system installs, and not from already existing servers.
7.15.2.	Any servers providing directory functions MUST be prevented from accessing the internet (or other untrusted networks) directly.
7.15.3.	Any servers providing directory functions MUST be protected by network security controls commensurate to the increased impact of their compromise.

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	TBD	N/A
DWP Patching Policy	TBD	N/A
DWP Approved File Systems	TBD	N/A

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.

11. Reference Documents

DWP Digital Blueprint

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

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.

12. Definition of Terms

Term	Definition
Lock	Prevent further actions being taken by an entity, without that entity re-presenting credentials.
Log Off	End an interactive session, where granted authorizations are relinquished or revoked.
Log On	Begin an interactive session, after some form of authentication. This can be username/password authentication, certificate based authentication, or others.
Server	In the context of this standard, a logical component that provides a service to other components. This consists of an operating system and an application, process, or service running on that system; and includes both virtualised and dedicated physical hardware.
Server Application	In this standard, this refers to the application, process or service that provides a service to other components. For example, NginX (a web server application)
Server Operating System	Any operating system upon which server applications are, or will be, installed. For the purpose of this standard, this includes specialist server operating systems (such as Windows Server 2016) as well as generic or desktop operating systems that are being used as servers.
Service Account	An account provisioned for use mainly or solely by applications or services rather than a human user.
User Account	An account provisioned for interactive use by human users.

13. Glossary

Abbreviation	Definition
DA	Design Authority
EAL4	Evaluation Assurance Level 4
EXT4	Extended (File System) 4
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell

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.

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-008 Server Operating System	**DWP Controls Catalogue - Baseline Control Set**	
Control Statement	**Control Reference**	**Descriptor**
10.1.1	-	-
10.1.2	-	-
10.1.3	-	-
10.2.1	-	-
10.2.2	-	-
10.2.3	-	-
10.2.4	-	-
10.2.5	-	-
10.3.1	-	-
10.3.2	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.
10.3.3	-	-
10.3.4	-	-
10.3.5	-	-
10.3.6	-	-
10.3.7	-	-
10.3.8	-	-
10.4.1	-	-
10.4.2	-	-
10.4.3	NT05	Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-

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-008 Server Operating System	**DWP Controls Catalogue - Baseline Control Set**	
		domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys.
10.4.4	-	-
10.4.5	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.
10.4.6	-	-
10.4.7	AC21	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
10.5.1	-	-
10.5.2	-	-
10.5.3	-	-
10.5.4	-	-
10.5.5	-	-
10.6.1	-	-
10.6.2	-	-
10.6.3	-	-
10.6.4	-	-
10.6.5	-	-
10.7.1	-	-
10.7.2	-	-
10.7.3	-	-
10.7.4	-	-
10.7.5	-	-
10.7.6	AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
10.7.7	AC14	Asset owners shall review users' access rights at regular intervals.
10.7.8	AC14	Asset owners shall review users' access rights at regular intervals.
	AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
10.7.9	-	-
10.7.10	-	-

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-008 Server Operating System	**DWP Controls Catalogue - Baseline Control Set**	
10.8.1	-	-
10.8.2	-	-
10.8.3	-	-
10.8.4	-	-
10.8.5	-	-
10.8.6	-	-
10.9.1	-	-
10.9.2	-	-
10.9.3	-	-
10.9.4	-	-
10.10.1	-	-
10.11.1	-	-
10.11.2	-	-
10.11.3	-	-
10.11.4	-	-
10.12.1	-	-
10.12.2	-	-
10.13.1	-	-
10.13.2	-	-
10.13.3	-	-
10.13.4	-	-
10.13.5	-	-
10.13.6	-	-
10.13.7	-	-
10.13.8	-	-
10.14.1	-	-
10.14.2	IN09	Information security incidents shall be responded to in accordance with the documented procedures.
10.14.3	-	-
10.14.4	-	-
10.14.5	-	-
10.15.1	-	-
10.15.2	-	-
10.15.3	-	-