Security Standard - Server Operating System (SS-008)

Chief Security Office

Department for Work & Pensions

Date: 15/05/2023

This Server Operating System 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	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision History

Version	Author	Description	Date
1.0		First published version	26/05/2017
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 11.1.1 Allow use of third-party patching solutions; Software versions still in support 11.1.2 CIS Benchmarks 11.1.3 Software inventory 11.2.1 Gold Builds 11.3.1 CIS Benchmarks; Gold Builds 11.3.2 Authority Reference (Master) Clock 11.3.8 Added reference to encryption standard 11.3.9 Vulnerability assessments 11.4.7 software versions 11.5.2 Added reference to firewall standard 11.5.5 Browsers and internet connection 11.6.3 Added reference to Access & Authentication standard 11.7.1 Added reference to privileged access control standard 11.7.2 Disable root access 11.7.7 Quarterly account checks, added reference to Access & Authentication standard 11.7.8 Added reference to Access & Authentication standard 11.8.7 Service account password rotation 11.8.8 Service account lockout 11.9.1 Added reference to Access & Authentication standard 11.9.4 Added reference to Access & Authentication standard	15/05/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	26/05/2017
2.0		Chief Security Officer	15/05/2023

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

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by first-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. O].
- independent external audit

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

5. Exceptions Process

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

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

This Server Operating System 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 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 v8 controls set. [see Appendix C 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 server operating systems are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with server operating systems, 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 v8 controls set. [see Appendix C 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 server operating systems deployments within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data. This includes specialist server operating systems (such as Windows Server) as well as generic or desktop operating systems upon which server applications will be, or are, installed.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

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 Operating System Selection

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Server operating systems **must** be of a version that is still under active vendor or extended third party support (including the use of third-party patching solutions where appropriate).	PR.DS-5 PR.MA-1
11.1.2	All servers **must** utilise an operating system that is secured and hardened in line with CIS benchmarks.	PR.IP-1
11.1.3	An inventory of all server operating systems installed on Authority assets **must** be maintained. The inventory must document the title, publisher, initial install/use date, and purpose for each entry deployment mechanism, and decommission date. This inventory **must** be reviewed at least bi-annually.	ID.AM-2

11.2 Installation

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Server operating systems **must** only be installed from a trusted source, utilising Gold Builds where available.	DE.CM-4
11.2.2	Server operating systems **must** only be connected to trusted networks during the install process.	PR.MA-1
11.2.3	Server operating system installations **must** include all current approved service packs / major releases for that operating system version.	PR.MA-1
11.2.4	Server operating system installations **must** apply all approved and verified updates and patches not already included on installation media immediately subsequent to installation.	PR.MA-1

11.3 General Configuration

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Security hardening baselines like CIS benchmarks **must** be used, and included in Gold Builds where appropriate.	PR.IP-1
11.3.2	Server operating systems **must** be configured to receive accurate time from the Authority Reference (Master) Clock, in compliance with SS-012 Protective Monitoring Security Standard [Ref. A]. Cloud based systems may use cloud providers' native time sources.	DE.AE-3
11.3.3	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.	PR.DS-2 PR.PT-3
11.3.4	Any operating system controls to protect system and application memory **must** be enabled.	PR.PT-4
11.3.5	Server operating systems **must** be configured so they do not auto-run inserted media.	PR.PT-3
11.3.6	Server operating systems **must** be patched in line with SS-033 Security Patching Standard [Ref. B].	PR.MA-1
11.3.7	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 SS-006 Security Boundaries Security Standard [Ref. C] and SS-018 Network Security Design Standard [Ref. D]).	PR.AC-5 PR.PT-4
11.3.8	All partitions containing configurations or sensitive data at rest must be encrypted according to SS-007 Use of Cryptography Security Standard [Ref. G].	PR.DS-1
11.3.9	Vulnerability assessments **must** be completed on a regular basis in line with the Technical Vulnerability Management Policy [Ref. P].	PR.IP-12

11.4 Applications and Services

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	All unnecessary applications, features and services **must** be disabled and removed where possible.	PR.PT-3
11.4.2	There **must** be measures in place to prevent installation of unauthorised applications or features onto servers.	PR.IP-3
11.4.3	Where possible, servers **must** be limited to performing one function only (such as web server, email server, file server, etc.).	PR.PT-3
11.4.4	All servers **must** have an anti-malware solution installed and operating, in line with SS-015 Malware Protection Security Standard [Ref. E].	DE.CM-4
11.4.5	Server applications **must** have their access to system resources limited to the minimum required to operate correctly.	PR.AC-4
11.4.6	Applications or services capable of circumventing or changing system controls **must** have their access restricted.	PR.AC-4
11.4.7	Server applications **must** be running versions that are still under active vendor support, maintained throughout their lifecycle, and **must** be patched according to SS-033 Security Patching Standard [Ref. B]. Out of date server applications that are not under active vendor support **must** be removed, or an approved exception in place (with an associated risk assessment).	PR.MA-1

11.5 Firewalls

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Server deployments **must** have a suitable host-based firewall configured and turned on (such as Windows Firewall, IPtables, etc.).	PR.PT-4
11.5.2	Servers **must** be deployed in a suitably protected location as defined by SS-018 Network Security Design Standard [Ref. D] and in line with SS-013 Firewall Security Standard [Ref. M].	PR.DS-5
11.5.3	Server firewalls **must** be set up to block all traffic by default, and only allow explicitly defined traffic.	PR.DS-2
11.5.4	Server firewalls **must** be configured to allow inbound or outbound traffic only on ports that are necessary to the operation of the system.	PR.DS-2
11.5.5	Servers **must** either have any internet browser applications (such as Edge) removed or disabled, or if a browser is required, it **must** not be able to access the internet.	PR.DS-5

11.6 Administration

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Server accounts **must** restrict administrative actions and access via Role-Based Access Control (RBAC) (such as through use of UAC or sudo).	PR.AC-4
11.6.2	Remote administration of servers **must** be carried out in accordance with the SS-016 Remote Access Security Standard [Ref. F].	PR.MA-2
11.6.3	All default passwords on all accounts must be changed, and comply with the DWP User Access Control Policy [Ref. J] and SS-001 pt.1 Access & Authentication Security Standard [Ref. H].	PR.AC-1
11.6.4	Administration of servers **must** be carried out from dedicated management infrastructure.	PR.MA-1

11.7 User Accounts

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	All server user accounts **must** be provisioned in accordance with the principle of least privilege and in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. N].	PR.AC-4
11.7.2	All server user accounts **must** enable individual users to be identified (e.g. unique accounts per user, or logged access to shared accounts). When feasible, root or admin accounts **must** be disabled.	DE.CM-3
11.7.3	Guest accounts **must** be removed.	PR.AC-4
11.7.4	Servers **must** implement measures to limit or prevent exposure of account names.	PR.DS-1
11.7.5	All servers **must** implement some form of account or session lock after no more than 10 failed login attempts. The form this takes (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.	PR.AC-2
11.7.6	User accounts on servers **must** be removed when they are no longer required.	PR.AC-1
11.7.7	User accounts on servers **must** be reviewed at least quarterly and be removed if they are no longer required, in line with SS-001 pt.1 Access & Authentication Security Standard [Ref. H].	PR.AC-1
11.7.8	User accounts on servers **must** be evaluated at least every six months to ensure the permissions assigned to them are still appropriate, in line with SS-001 pt.1 Access & Authentication Security Standard [Ref. H].	PR.AC-1
11.7.9	Revoked or disabled accounts **must** only be re-issued to the individual that the account is currently assigned to.	PR.AC-1
11.7.10	User accounts **must** automatically terminate user sessions (either by logging off or locking) after being inactive for no more than 10 minutes.	PR.AC-2

11.8 Service Accounts

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	All server service accounts **must** be provisioned in accordance with the principle of least privilege.	PR.AC-4
11.8.2	Service accounts **must** be unique accounts that are not shared with human users.	PR.AC-1 PR.AC-4
11.8.3	Service accounts **must** limit the number of services that access them.	PR.PT-3
11.8.4	Service accounts **must** have interactive login disabled.	PR.PT-3
11.8.5	Service accounts on servers **must** be removed when they are no longer required.	PR.PT-3
11.8.6	Service accounts on servers **must** be reviewed at least every six months, and be removed if they are no longer required.	PR.AC-1
11.8.7	Service account passwords **must** be changed in line with NCSC guidance on password management and with SS-001 pt.1 Access and Authentication Security Standard [Ref. H].	PR.AC-1 PR.AC-4
11.8.8	Service accounts **must** be disabled after 3 invalid login attempts. The account **must** be disabled for an escalating time interval, minimum time of 15 minutes, sufficient to discourage brute force guessing of credentials, but not so long as to allow for a denial-of-service attack to be performed.	PR.AC-1 PR.AC-4

11.9 Authentication Credentials

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	All passwords used on servers **must** be compliant with the requirements of the DWP User Access Control Policy [Ref. J] and SS-001 pt.1 Access & Authentication Security Standard [Ref. H].	PR.AC-6
11.9.2	Credentials **must** be stored and protected in line with SS-007 Use of Cryptography Security Standard [Ref. G].	PR.DS-1
11.9.3	Credentials for operating system accounts **must** be unique per account.	PR.AC-1 PR.AC-6
11.9.4	Server operating systems must have technical controls implemented to ensure passwords assigned to human users have appropriate lifetimes, in compliance with the DWP User Access Control Policy [Ref. J] and SS-001 pt.1 Access & Authentication Security Standard [Ref. H].	PR.AC-1

11.10 Physical Access Control

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	Physical access to hardware hosting any server operating system **must** be restricted appropriately in accordance with the DWP Physical Security Standard [Ref. K].	PR.AC-2

11.11 Logical Access Control

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Servers **must** be compliant with the SS-001 pt.1 Access and Authentication Security Standard [Ref. H].	PR.AC-4
11.11.2	Servers **must** ensure access to system resources is authorised appropriately.	PR.AC-4
11.11.3	Servers **must** require credentials when waking from sleep, hibernation, or suspended operation.	PR.AC-6
11.11.4	Servers **must** prevent remote access to Plug and Play (PNP) services.	PR.AC-3

11.12 Backup

Reference	Minimum Technical Security Measures	NIST ID
11.12.1	Servers **must** be backed up in accordance with SS-035 Backup and Restore Security Standard [Ref. I].	PR.IP-4
11.12.2	Server backups **must** prevent access to application data without the appropriate cryptographic keys.	PR.DS-1

11.13 System Logging

Reference	Minimum Technical Security Measures	NIST ID
11.13.1	All logging carried out on servers **must** be conducted in accordance with SS-012 Protective Monitoring Security Standard [Ref. A].	PR.PT-1
11.13.2	All logs produced on servers **must** be forwarded to the appropriate centralised log collection point, in compliance with SS-012 Protective Monitoring Security Standard [Ref. A].	DE.DP-4
11.13.3	All attempts to change server configurations **must** be logged.	DE.CM-7
11.13.4	Any events which involve privilege escalation **must** be logged.	DE.CM-7

11.13.5	Log on / log off events **must** be logged.	DE.CM-3
11.13.6	Actions that modify or create users or groups, or modify the privileges of users or groups on servers, **must** be logged.	DE.CM-3
11.13.7	Shutdown and system suspension events on servers **must** be logged.	DE.CM-7
11.13.8	Failed object access or privilege use **must** be logged.	DE.CM-7

11.14 Monitoring and Alerting

Reference	Minimum Technical Security Measures	NIST ID
11.14.1	Alerts **must** be generated in accordance with SS-012 Protective Monitoring Security Standard [Ref. A].	DE.DP-4
11.14.2	Processes invoked in response to alerts **must** be compliant with the Security Incident Management Policy [Ref. L].	DE.DP-2
11.14.3	Alerts **must** be generated for any events that would prevent core server functionality	DE.DP-4
11.14.4	Alerts **must** be generated for any event or combination of events that is indicative of unusual user or process activity.	DE.DP-4
11.14.5	Failed authentication events **must** generate an alert.	DE.DP-4

11.15 Directory Servers

Reference	Minimum Technical Security Measures	NIST ID
11.15.1	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.	PR.IP-1
11.15.2	Any servers providing directory functions **must** be prevented from accessing the internet (or other untrusted networks) directly.	PR.PT-4
11.15.3	Any servers providing directory functions **must** be protected by network security controls commensurate to the increased impact of their compromise.	PR.PT-4

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
ID.AM-2	Physical devices and systems within the organization are inventoried	11.1.3
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.6.3, 11.7.6,11.7.7, 11.7.8, 11.7.9, 11.8.2, 11.8.6, 11.8.7, 11.8.8, 11.9.3, 11.9.4
PR.AC-2	Physical access to assets is managed and protected	11.7.5, 11.7.10, 11.10.1
PR.AC-3	Remote access is managed	11.11.2
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.4.5, 11.4.6, 11.6.1, 11.7.1, 11.7.3, 11.8.1, 11.8.2
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.3.7
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.9.1, 11.9.3, 11.11.3
PR.DS-1	Data-at-rest is protected	11.3.8, 11.7.4, 11.9.2, 11.12.1
PR.DS-2	Data-in-transit is protected	11.3.3, 11.5.3, 11.5.4
PR.DS-5	Protections against data leaks are implemented	11.1.1, 11.5.2, 11.5.5

PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	11.1.2. 11.3.1, 11.15.1
PR.IP-3	Configuration change control processes are in place	11.4.2
PR.IP-4	Backups of information are conducted, maintained, and tested	11.12.1, 11.15.2, 11.15.3
PR.IP-12	A vulnerability management plan is developed and implemented	11.3.9
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.1.1, 11.2.2, 11.2.3, 11.2.4, 11.3.6, 11.4.7, 11.6.4
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	11.6.2
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.13.1
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.3.3, 11.3.5, 11.4.1, 11.4.3, 11.8.3, 11.8.4, 11.8.5
PR.PT-4	Communications and control networks are protected	11.3.4, 11.3.7, 11.5.1, 11.11.1, 11.11.2
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.3.2
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	11.7.2, 11.13.5, 11.13.6
DE.CM-4	Malicious code is detected	11.2.1, 11.4.4

DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.13.3, 11.13.4, 11.13.7, 11.13.8
DE.DP-2	Detection activities comply with all applicable requirements	11.14.2
DE.DP-4	Event detection information is communicated	11.13.2, 11.14.1,11.14.3, 11.14.4, 11.14.5

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-012 Protective Monitoring Security Standard	Yes
B	SS-033 Security Patching Standard	Yes
C	SS-006 Security Boundaries Security Standard	Yes
D	SS-018 Network Security Design Standard	Yes
E	SS-015 Malware Protection Security Standard	Yes
F	SS-016 Remote Access Security Standard	Yes
G	SS-007 Use of Cryptography Security Standard	Yes
H	SS-001 pt.1 Access and Authentication Security Standard	Yes
I	SS-035 Backup and Restore Security Standard	Yes
J	DWP User Access Control Policy	Yes
K	Physical Security Standard	Yes
L	Security Incident Management Policy	TBA
M	SS-013 Firewall Security Standard	Yes
N	SS-001 pt.2 Privileged User Access Security Standard	Yes
O	Security Assurance Strategy	No
P	Technical Vulnerability Management Policy	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 National Institute of Standards and Technology Cyber Security Framework
OWASP Open Web Application Security Project

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
DDA	Digital Design Authority
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
RADIUS	Remote Authentication Dial In User Service
SSH	Secure Shell

Appendix E Definition of Terms

Table 5 – Glossary

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 authorisations 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) 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.
Lock	Prevent further actions being taken by an entity, without that entity re-presenting credentials.

Appendix F Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps