Security Standard - Desktop Operating System (SS-010)

Chief Security Office

Date: 22/03/2023

Department for Work & Pensions

This Desktop 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	18/09/2017
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 • Compliance changed to Security Assurance • Scope amended to include laptop devices • 11.1.1 Added reference to Use of Cryptography standard • 11.1.2 Added reference to Remote Access standard • 11.1.3 secure enterprise connection • 11.2.1 Clarified on-device data; Updated NCSC reference • 11.2.3 Reference added to Secure Sanitisation standard • 11.3.5 Reference added to server OS standard • 11.5 Whitelisting changed to allowlisting • 11.5.1 Including engineering devices • 11.5.3 Use of mobile device management system • 11.6.3 Reference added for patching standard; out of date software must be removed • 11.6.4 Endpoint controls • 11.7.1 Security baselines / CIS Benchmarks • 11.8.3 Allowlist; IKEv2 • 11.10.4 Reference added to Authority Master Clock and cloud providers time sources • 11.12.1 Reference added to Secure Sanitisation standard • 11.13.1 Exception added for cloud first devices; Reference added to Wireless Network standard • 11.14.1 Reference added to Security Patching standard	22/03/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	22/03/2023

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. M].
- 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 Desktop 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 (see Appendix C for full list external references) 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 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 desktop operating systems are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with desktop 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 desktop (and laptop [including engineering devices] where applicable) operating systems deployments, both physical and virtual, within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data. Where the term 'desktop' is used, the security measures also apply to laptop and engineering devices, with appropriate caveats used where necessary.

For any desktops accessing non-production environments, this **must** be clearly indicated on the screen via a flag, banner or other indicator so that users are clear on what they are accessing.

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 Assured Data in Transit

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Data **must** be protected as it transits between the Desktop and any connecting service(s), in line with SS-007 Use of Cryptography Security Standard [Ref. B].	PR.DS-2
11.1.2	A VPN solution **must** be implemented according to SS-016 Remote Access Security Standard [Ref. J].	PR.DS-2
11.1.3	All network data from the desktop **must** be routed over an agreed secure enterprise connection (e.g. VPN) when working remotely.	PR.DS-2
11.1.4	An assured firewall solution **must** be used in compliance with SS-013 Firewall Security Standard [Ref. A] and configured to block outbound traffic when the VPN is not active.	PR.DS-5
11.1.5	Where certificates provide user or machine credentials, they **must** be used and these credentials should bind to the device's hardware.	PR.AC-6

11.2 Assured Data at Rest

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Data should not be stored on the device, but on network shared storage, however data that must persist on the device such as temporary / cached or offline data (including any attached removable storage) **must** be satisfactorily encrypted when at rest (or when locked for always-on devices). The device **must** be configured to provide full volume encryption using an assured / approved data-at- rest encryption product, although application level encryption is not required.	PR.DS-1

	Assurance of this function is necessary that takes account of NCSC Device Security Guidance and SS-007 Use of Cryptography Security Standard [Ref. B].	
11.2.2	A Trusted Platform Module (TPM 2.0 hardware chip for laptop devices for example) can be used in place of a token where the deployment environment risks allow, making the user's experience smooth whilst providing a similar degree of cryptographic strength to the Smart Token method.	PR.DS-1
11.2.3	Devices containing data **must** be disposed of securely according to SS-036 Secure Sanitisation and Destruction Security Standard [Ref. H].	PR.DS-3 PR.IP-6

11.3 Authentication

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Each of the three types of authentication described **must** be implemented: • User to desktop: Authenticating to the device in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. C], the user is only granted access to the desktop after successfully authenticating to the desktop. • User to service: The user is only able to access enterprise services after successfully authenticating to the service, via their desktop. Access via remote services requires successfully authenticating to the service, via authorised device types. • Desktop to service: Only Authority authorised desktops which can authenticate to the enterprise can be granted access.	PR.AC-1 PR.AC-7
11.3.2	There **must** be authentication to both the encryption product i.e. to access the encrypted drive and the OS platform.	PR.AC-1 PR.AC-7
11.3.3	All default passwords **must** be changed and password configuration parameter options set in accordance with DWP User Access Control Policy [Ref I].	PR.AC-6

11.3.4	Use of Biometric authentication factors is preferred, and **must** be in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. C].	PR.AC-6
11.3.5	System administration privileged accounts **must** only be used on desktops deployed to perform administrative function. Such privileged user accounts with administrative privileges **must** deploy strong authentication including a second factor to authenticate to the platform at both logon and unlock time in compliance with SS-001 pt.2 Privileged User Access Security Standard [Ref. D]. See SS-008 Server Operating System Security Standard [Ref. K] for more detail on systems administration.	PR.AC-4 PR.AC-6

11.4 Secure Boot

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	An unauthorised entity **must** not be able to modify the boot process of a desktop, and any attempt to do so **must** be detected, where suitable mechanisms exist.	PR.IP-3 DE.DP-4
11.4.2	Due to the platform specific vendor protection methods available, a risk assessment of the vendor secure boot implementation guidance **must** confirm if the platform meets the Authority's protective security requirements.	ID.RA-1
11.4.3	Users **must** be educated to recognise and report where suspicion is that the boot process has been compromised.	PR.AT-1

11.5 Application Allowlisting

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	An allowlist of authorised applications (including those utilised on engineering devices) **must** be defined and maintained.	ID.AM-1 PR.IP-1
11.5.2	Arbitrary application installation by users **must** not be allowed.	PR.IP-3
11.5.3	Authorised application deployment **must** only be performed by an administrator using a trusted mechanism, e.g. a mobile device management system.	PR.IP-3

11.6 Malicious Code

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	All Desktop operating systems **must** implement capability to detect, isolate and defeat malicious code which becomes present on the device. The selection of appropriate countermeasures is to be informed by a per platform risk assessment selection. This **must** include platform specific recommendations for Malware Threat countermeasures and in combination include:- • Anti-malware tools; • Behavioural monitoring of applications and platform; • File and URL reputation.	DE.CM-4
11.6.2	There **must** be an agreed anti-malware solution deployed on the desktop endpoint that deploys established product(s) in line with SS-015 Malware Protection Security Standard [Ref. E]	DE.CM-4
11.6.3	Desktop software **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. F]. Out of date software that is not under active vendor support **must** be removed, or an approved exception in place (with an associated risk assessment).	PR.DS-3 PR.MA-1
11.6.4	Content-based attacks **must** be filtered by Endpoint controls on the device.	DE.CM-4

11.7 Security Policy Enforcement

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Security baselines (e.g. CIS Benchmarks or similar) **must** be used to help define operating system security policies. Any deviations from standard configurations **must** be documented.	PR.IP-1
11.7.2	Only privileged users with specific change control authorisation **must** be able to override or modify Security Group Policy.	PR.AC-4
11.7.3	Security policies **must** be enforced. A combination of operating system and third-party product configuration specific to the platform can meet requirements.	ID.GV-1
11.7.4	Mobile Device Management (MDM) profiles **must** be marked as non-removable so the user cannot remove them and alter their configuration.	PR.DS-5

11.8 External Interface Protection

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	The desktop **must** be able to constrain the set of ports available and **must** be hardened and robust to malicious attack.	PR.PT-4
11.8.2	Network interface protection **must** include a host based firewall configured to prevent inbound initiated network connections to the device and limiting outbound connection to the Authority's IPsec VPN gateway (or other approved solution e.g. IKEv2) only, on the required ports, where external connection is required.	PR.PT-4
11.8.3	Physical and wireless interfaces **must** only allow an allowlist of authorised peripherals or peripheral classes to connect and communicate with the desktop, additionally connection **must** only use specific protocols. Subject to risk assessment, interface configuration **must** block unauthorised external devices e.g. USB removable media or configured to read-only, to limit data import and export where business requirements exist.	PR.PT-4

11.8.4	Direct Memory Access (DMA) **must** be restricted from external interfaces. Where the OS platform does not control access via DMA it is advisable to procure hardware which does not have external DMA interfaces present.	PR.PT-4
11.8.5	All exports to the Internet **must** be authorised by and traceable to a user.	PR.PT-1 DE.CM-3

11.9 Device Policy Update

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	The Enterprise solution (whether on premise or in the Cloud) **must** be able to issue security updates and remotely validate the patch level of all authorised desktop endpoint device types across the entire estate.	PR.MA-1
11.9.2	The appropriate version/patches for the OS **must** be downloaded and installed in accordance with SS-033 Security Patching Security Standard [Ref. F].	PR.MA-1
11.9.3	There **must** be controls implemented to audit, monitor, (and as functionally available per desktop device specific), enforce updates of the OS platform, system firmware and any appropriate applications.	PR.MA-1 PR.PT-1

11.10 Event Collection for Enterprise Analysis

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	The Enterprise solution (whether that is on premise or in cloud based systems) **must** be able to report security-critical events to the Authority's Enterprise SOC audit and monitoring service for all authorised desktop device types and services in line with SS-012 Protective Monitoring Security Standard [Ref. G].	DE.AE-3 DE.CM-1

11.10.2	Security critical events which can **only** be collected from the desktop are required to be logged, as collecting audit events from enterprise services is preferred where possible and duplication of event collection should be avoided. Desktop logging includes (not an exhaustive list) e.g.:- • User log in and log out • Local security alerts from third party tools or platform components such as alerts from anti-malware, host-based firewall, platform integrity checks which fail.	DE.AE-3
11.10.3	Event collections **must** be implemented using an appropriate assessed solution. Users **must** be prevented from log tampering and ensure the integrity of the reporting service is protected. Risk assessment **must** be used to determine the requirement for viewing both locally and remotely.	DE.AE-3
11.10.4	Accurate time stamps are required for audit and time on devices should be synchronised to the Authority's Reference (Master) Clock, maintained via an NTP hierarchy. For cloud based systems, the cloud providers' time services are sufficient for time reference synchronisation, as the Authority does not have reliable means to share Authority Master Clock data with external parties.	DE.DP-2

11.11 Incident Response

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Authority desktop devices **must** have configurable capability to support the Authority's Enterprise incident handling and response plans. Appropriate desktop functionality includes:- • Desktop to be locked, wiped, and configured remotely; • Sending a wipe command to the desktop and revoking credentials; • Remote function to destroy encryption key material or using secure erase functions if the device is present	PR.DS-5
11.11.2	The enterprise **must** be able to revoke user credentials and / or access to Authority network by revoking both the VPN client and any other enterprise services certificates e.g. e-mail that are stored on the desktop whenever a compromise is suspected.	PR.AC-1

11.12 Desktop Device Sanitisation and Re-Provisioning

Reference	Minimum Technical Security Measures	NIST ID
11.12.1	SS-036 Secure Sanitisation and Destruction Security Standard [Ref. H] **must** be applied before Authority endpoint devices are released outside of the Authority.	PR.DS-3 PR.IP-6
11.12.2	Where deploying or redeploying Authority endpoint devices within a Authority Security management boundary domain, platform specific guidance **must** be defined under risk assessment agreement to restore a misconfigured or potentially compromised device to a known good state using native functionality. Scenarios include:- • Sanitising device believed to be compromised with malware; • Preparing a device which has not previously been managed; • Reissuing device to a different user in the same security environment.	PR.DS-3 PR.MA-1

11.13 Wi-Fi

Reference	Minimum Technical Security Measures	NIST ID
11.13.1	Where appropriate, Authority desktop devices **must** be configured to maintain always-on Authority VPN when not connected to the Authority LAN Infrastructure and Internet is available. This requirement does not apply to 'Cloud First' devices that do not utilise standard VPN infrastructure. Please refer to SS-019 Wireless Network Security Standard [Ref. L] for further information.	PR.DS-2

11.14 Browsers

Reference	Minimum Technical Security Measures	NIST ID
11.14.1	Authority desktop devices **must** deploy a mature and secure browser product that is in support and maintains a hardened build that takes advantage of the native security features of the underlying platform and remains compliant with SS-033 Security Patching Security Standard [Ref. F].	PR.DS-5

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-1	Physical devices and systems within the organization are inventoried	11.5.1
ID.GV-1	Organizational cybersecurity policy is established and communicated	11.7.3
ID.RA-1	Asset vulnerabilities are identified and documented	11.4.2
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.3.1, 11.3.2, 11.11.2
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.3.5, 11.7.2
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.1.5, 11.3.3, 11.3.4, 11.3.5
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.3.1, 11.3.2
PR.AT-1	All users are informed and trained	11.4.3
PR.DS-1	Data-at-rest is protected	11.2.1, 11.2.2

PR.DS-2	Data-in-transit is protected	11.1.1, 11.1.2, 11.1.3, 11.13.1
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	11.2.3,11.6.3, 11.12.1, 11.12.2
PR.DS-5	Protections against data leaks are implemented	11.1.4, 11.7.4, 11.11.1, 11.14.1
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)	11.5.1, 11.7.1
PR.IP-3	Configuration change control processes are in place	11.4.1, 11.5.2, 11.5.3
PR.IP-6	Data is destroyed according to policy	11.2.3, 11.12.1
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.6.3, 11.9.1, 11.9.2, 11.9.3, 11.12.2
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.8.5, 11.9.3
PR.PT-4	Communications and control networks are protected	11.8.1, 11.8.2, 11.8.3, 11.8.4
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.10.1, 11.10.2, 11.10.3
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.10.1
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	11.8.5
DE.CM-4	Malicious code is detected	11.6.1, 11.6.2, 11.6.4

DE.DP-2	Detection activities comply with all applicable requirements	11.10.4
DE.DP-4	Detection processes are continuously improved	11.4.1

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-013 Firewall Security Standard	Yes
B	SS-007 Use of Cryptography Security Standard	Yes
C	SS-001 pt.1 Access and Authentication security standard	Yes
D	SS-001 pt.2 Privileged User Access Security Standard	Yes
E	SS-015 Malware Protection Security Standard	Yes
F	SS-033 Security Patching Security Standard	Yes
G	SS-012 Protective Monitoring Security Standard	Yes
H	SS-036 Secure Sanitisation and Destruction Security Standard	Yes
I	DWP User Access Control Policy	No
J	SS-016 Remote Access Security Standard	Yes
K	SS-008 Server Operating System Security Standard	Yes
L	SS-019 Wireless Network Security Standard	Yes
M	Security Assurance Strategy	No

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
NCSC Device Security Guidance

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
DWP	Department for Work and Pensions (DWP)
DA	Design Authority (DA)
DMA	Direct Memory Access
IPsec	Internet Protocol Security
ITHC	IT Health Check
LAN	Local Area Network
MDM	Mobile Device Management
NCSC	National Cyber Security Centre
NTP	Network Time Protocol
OS	Operating System
TPM	Trusted Platform Module
USB	Universal Serial Bus
VPN	Virtual Private Network

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Captive portal	A web page that the user of a public-access network is obliged to view and interact with before access is granted.
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).
Data sanitisation	The process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device.
Firewall	Type of security barrier placed between network environments consisting of a dedicated device or a composite of several components and techniques through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass.
Malware	Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.
Security Group Policy	Provides centralized management and configuration of operating systems, applications, and users' settings
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

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