Security Standard – Malware Protection (SS-015)

Chief Security Office

Date: 21/01/2025

Department for Work & Pensions

This Malware Protection Security Standard is part of a suite of standards, designed to promote consistency across the Authority, 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.

Security standards and policies considered appropriate for public viewing are published here:

Government Publications 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).

(Important note for screen reader users.) Paragraphs that contain a 'must' statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

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	20/03/2017
2.0		Full update in line with current best practices and standards; Updated Intro, purpose, audience, scope Written to be vendor and technology agnostic as far as possible to increase applicability Replaced use of technical control requirements to minimum security measures Re-formatted document to categorise security measures under 15 headings. Added NIST sub-category references against each security measure Added new table in Appendix A which list security outcomes the measures support the achievement of Updated references and included links to external publications etc. 11.1.2 Updated regarding use of open source anti-malware 11.2 New section for privileged users 11.5.2 Added caveat for special users 11.8.1 File transfer restrictions in instant messaging 11.10.3 Requirement added for sandboxing 11.13.5 Block C&C traffic	09/02/2023

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years Intro – NCSC advice; agentless malware protection 11.1.1 Next generation tools 11.1.2 Definition of assets and SLAs for open source tools 11.1.3 & 11.1.4 Data flow scanning and type of traffic 11.1.5 Legitimate software used for malware 11.1.6 Emerging programming languages used for malware 11.2.2 & 11.2.3 Non-human and service accounts 11.3.2 Software configuration control; reference added to Patching Standard 11.5.3 Reworded for clarity 11.6.2 Automated sandboxing; Offline checking of media 11.7.1 Authentication enforcement 11.7.2 Or equivalent 11.8.1 Internal/external file sharing; executable files 11.9.2 Allow listing 11.9.3 Configuration control 11.9.4 Security Incidents 11.9.5 Testing 11.9.6 Software inventory 11.10.3 Inline scanning; Sandboxing initial analysis only 11.12.5 Incidents 11.12.9 Next generation tools	21/01/2025

		11.13 Allow listing and block listing 11.13.7 Must where possible 11.13.8 API based cloud sandboxing techniques 11.13.9 API-based email content detection and response capabilities External references – NCSC Mitigating malware and ransomware attacks	

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	09/02/2023
2.1		Chief Security Officer	21/01/2025

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

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

- controls tests performed by 1st 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.
- independent external audit

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

5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

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 that require malware protection.

7. Accessibility Requirements

(Important) this paragraph contains ‘must’ activities.

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

8. Introduction

(Important) this section contains ‘must’ activities.

This Malware Protection Security Standard provides the list of security measures that are required to secure Authority User Access Devices, Servers and infrastructure components to an Authority approved level of security. This standard provides a list of security measures to protect citizen and operational data to be stored or processed in order to minimise the risk from known threats both physical and logical to an acceptable level for operations.

Quoting NIST (National Institute of Standards and Technology) the definition of malware is:

“Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose."

NCSC have stated that it is not possible to completely protect an organisation against malware infection, and advise that a 'defence-in-depth' approach is adopted using layers of defence with several mitigations at each layer. Organisations will have more opportunities to detect malware, and then stop it before it causes real harm to the organisation. [See External References - NCSC Mitigating malware and ransomware attacks].

There are several use cases requiring malware controls and agent-based and agentless malware mitigation software that **must** be considered on all End User Devices, e.g., desktop endpoints, mobile end points, along with all server end points (physical and virtual including Hypervisor) and at the content inspection and inline infrastructure layers.

Malware detection capability **must** be considered on webserver end points, mail server endpoints, remote access servers / VPN concentrators, firewalls, proxy and reverse proxy servers and intrusion prevention systems.

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 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 malware controls are implemented consistently across the Authority and its third-party service providers.
- Mitigate risks from the threats and vulnerabilities associated with malware 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 set. [see 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

(Important) this paragraph contains ‘must’ activities.

This standard applies to systems deployed to meet the Authority’s business objectives. All endpoints **must** have Anti-Malware software based agents installed to help protect against and remediate infection, and **must** meet all the requirements in this standard. The scope includes endpoints that receive auxiliary agentless anti-malware mitigation via IDS / IPS, Next Generation Sandboxing devices, and other Content Inspection devices, which **must** meet all of the logging and incident handling requirements. Any devices that are not anti-malware compatible **must** be protected by suitable compensating controls. Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains ‘must’ activities.

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. Malware Protection Security Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	When selecting Anti-Malware software and Anti-Malware Content Inspection devices during both procurement and deployment, architects **must** evaluate Anti-Malware technologies that provide similar functionality throughout the end-to-end systems architecture and select products to avoid duplication of identical scanning engines and to remove unnecessary performance overhead. Consideration **must** be given to the use of Next Generation products (including AI and machine learning capabilities), given that sophisticated malware is becoming more difficult for current signature-based products to detect.	n/a
11.1.2	If open-source Anti-Malware software is chosen, clear SLA’s and escalation processes **must** be defined to handle software failure, i.e., signature updates that may cause false positives and impact associated systems and service operating. (Note: Commercially available Anti-Malware will have well-defined Service Level Agreements as part of the procurement and commercial contract. Open-source Anti-Malware software will not necessarily have these in place by default, but **must** have a clearly defined service wrapper in place, including a definition of assets and Service Level Agreements, supported by commercial agreements where appropriate.)	GV.OC-05

Reference	Minimum Technical Security Measures	NIST ID
11.1.3	All data flows **must** include details of protocols used, and source and destination IP addresses or URLs and be recorded in a High Level Design or other architectural documentation. All data flows **must** consider type of traffic including any file transfers allowed.	ID.AM-03
11.1.4	Data flows **must** be monitored to identify any unusual or suspicious events that could indicate the presence of malware, with on access scanning for any file download and scanning at the gateway.	DE.CM-01
11.1.5	Threat actors are increasingly using native or legitimate software such as RDP, SSH and file transfer tools to carry out attacks in order to evade detection and blend in with normal business traffic. Malware protection capabilities **must** be in place to detect any anomalous patterns or behaviour in these tools for further analysis.	DE.CM-01 DE.CM-09
11.1.6	Similarly, threat actors are also starting to use emerging programming languages, which can leverage cross-platform capabilities and are better at evading anti-virus and ageing security tools. Malware protection capabilities **must** be kept up to date to keep abreast of novel languages and new techniques, in line with SS-033 Security Patching Standard [Ref. B].	PR.PS-02

11.2. Privileged Users

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Privileged Users who manage Anti-Malware software, hardware, processes and services **must** be able to demonstrate having the appropriate level of training for the products, processes and services they manage.	PR.AT-02
11.2.2	Privileged Users **must** be managed in accordance with SS-001 pt.2 Privileged User Access Security Standard [Ref. C]. This also applies to non-human or service accounts.	PR.AA-05
11.2.3	The principle of least privilege **must** be applied to ensure that end users (including non-human and service accounts) only have the required access to perform their business tasks and no access to modify any system parameters on the Operating System other than for HID (Human Interface Devices) e.g., for their personal ergonomic requirements. This includes but is not limited to restricting access to system logs, driver settings, time settings, host-based firewalls, process browsers, and service management settings. Full coverage of desktop / end user operating system lockdown can be found in SS-010 Desktop Operating System Security Standard [Ref. A].	PR.AA-05

11.3. Operating System

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Operating Systems **must** be running versions that are still under active vendor support and must be patched under time sensitive operating procedures according to SS-033 Security Patching Standard [Ref. B].	ID.AM-08 PR.PS-02
11.3.2	All operating system software **must** be under configuration control and patched in line with SS-033 Security Patching Standard [Ref. B], with procedures in place to monitor for out of date or obsolete software installed on the infrastructure. If an Operating System is in use that is no longer under vendor support, a clear migration plan **must be** well-defined and managed. Furthermore, other mitigations to ensure clear restrictions to Internet based traffic and an adequate level of inline Content Inspection **must** be in effect. (This is because end point Anti-Malware software on these systems will not provide the required level of protection).	ID.AM-02 PR.PS-02 PR.IR-01

11.4. Anti-malware Software

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Standard business users **must not** have any access to modify or disable the scanning parameters of the Anti-Malware software. This includes preventing user access to disable Anti-Malware capabilities in the BIOS.	PR.AA-05 PR.IR-01
11.4.2	Access to the Anti-Malware software console **must** be protected to avoid any tampering by non-privileged users.	PR.AA-05 PR.IR-01
11.4.3	Any privileged access exercised to modify Anti-Malware software scanning parameters **must** be fully logged and audited.	PR.PS-04 PR.AA-05

11.5. Browser

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.5.1	Standard business users **must not** have any access to modify any of the browser-based settings such as, but not limited to, privacy settings, proxy settings, Active X, and Java based settings.	PR.AA-05
11.5.2	Standard business users **must not** have the ability to install or modify any browser-based plugins. Non-production users (e.g. engineers, developers etc.) may install plugins via a request/approval process.	PR.AA-05

11.5.3	Standard business users **must** only have access to browser-based parameters for the accommodation of ergonomic requirements such as modifying the zoom feature for vision assistance.	PR.AA-05
11.5.4	Configuration on the browser **must** severely limit non-essential browsing features such as web-based popups and iFrames; any requirement or exception **must** be subject to security assessment and accordingly authorised.	PR.AA-05
11.5.5	Users **must**: i) only use corporately approved browsers, ii) NOT have the ability to install any non-approved browsers This is a specific clause to item 11.9.1.	PR.AA-05 PR.PS-05

11.6. Removable Storage

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.6.1	If removable media is authorised as part of legitimate business use, the auto-run feature **must** be disabled and an on demand Anti-Malware software scan **must** be completed and successfully passed prior to the data being persisted on department systems.	PR.DS-01
11.6.2	Removable media is enabled for Read Only access, but Write access is only enabled with the correct authorisation. Automated sandboxing **must** be in place where appropriate; air-gapped sandboxing **must** be in place for Operating System or infrastructure files; Offline checking of media **must** be carried out before media is allowed on devices and endpoints.	PR.DS-01

11.7. Virtual Private Network

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.7.1	Any VPN Concentrators aggregating remote worker access to systems and services implemented for Authority business and services **must** perform a posture check of the devices attempting remote connectivity. This **must** include checks on patching levels, Anti-Malware software signature levels Anti-Malware software service status and confirmation that the device is appropriately authorised and authentication has been enforced to access the network.	PR.AA-03 PR.DS-02
11.7.2	If remote worker end point devices do not meet posture check requirements of the VPN concentrator (or equivalent), there **must** be an effective facility in a quarantine / staging area to rectify patching levels, Anti-Malware software signature levels and service status in order to reattempt successful connection.	PR.DS-02

11.8. Instant Messaging

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.8.1	Only approved Instant Messaging channels may be used for sharing files within the Authority, and only enabled for authorised and approved external participants. Executable files **must not** be shared via instant messaging channels.	PR.PS-05
11.8.2	If communicating with approved federated third parties via an Instant Messaging channel, file transfer **must** have an on-demand Anti-Malware software scan enabled	PR.IR-01

11.9. General Software Controls

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.9.1	Standard business users **must not** have the ability to install unauthorised software on any departmental systems.	PR.PS-05
11.9.2	Endpoint controls **must** consider application allow listing to help mitigate the deployment of unauthorised software and malware execution.	PR.PS-05
11.9.3	All approved software **must** be subject to the same patching standards as the underlying Operating System, and in line with SS-033 Security Patching Standard [Ref. B]. All software **must** be under configuration control and monitored to ensure it is up to date.	PR.PS-02

Reference	Minimum Technical Security Measures	
11.9.4	Any software found to have bypassed any control mechanisms for installation **must** be automatically disabled / quarantined and subjected to a formal review and uninstallation if deemed necessary. A security incident must also be raised as per SS-014 Security Incident Management Standard [Ref. E].	PR.PS-02
11.9.5	All approved software to be installed **must** be tested prior to deployment on devices and endpoints.	ID.RA-09
11.9.6	An inventory of software **must** be maintained to support hardening of devices and endpoints.	ID.AM-02

11.10. File Transfer Controls

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	
11.10.1	File Transfers **must** be subject to at least one layer of content inspection by Anti-Malware software prior to the data being resident/ persistent on department systems	DE.CM-01
11.10.2	File Transfers with approved third parties **must** be subject to at least two layers of content inspection. Where decryption is possible, this **must** be done firstly by a Security Boundary service, such as a Next Generation Firewall, Web Application Firewall, or Proxy Server, and secondly by a real time scan using the Anti-Malware software on the target end point.	DE.CM-01 DE.CM-06

Reference	Minimum Technical Security Measures	
11.10.3	All communication paths **must** be protected against malware with inline scanning or the capability to decrypt and inspect before delivering to its destination. Where file transfers are encrypted and cannot be decrypted for inspection in transit (e.g. certificate pinned files), these **must** be directed to a quarantine or sandbox environment, although it should be noted that this action could be limited to an initial analysis only.	PR.PS-05

11.11. Threat Intelligence

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	
11.11.1	Anti-Malware threat intelligence feeds **must** be regularly collected and reviewed from known, trusted third parties. These **must** be digested by a dedicated team and distributed to relevant stakeholders for consumption.	ID.RA-02 ID.RA-03 DE.AE-07

11.12. Anti-Malware Software for End Point Agents

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	
11.12.1	Anti-Malware software **must** be installed, verified and actively running on all end points.	DE.CM-01 DE.CM-06
11.12.2	Anti-Malware software **must** have on-access (real-time) scanning enabled by default for general web browsing, file and folder download and upload via email attachments.	DE.CM-01 DE.CM-06
11.12.3	Anti-Malware software **must** have as a minimum frequency interval a weekly on-demand scan completed of the entire file and folder structure. This **must** include a scan of the start-up files, boot records and memory.	DE.CM-01 DE.CM-06
11.12.4	Where exceptions are identified, conflicts with on-access (real-time) Anti-Malware and / or on-demand scans **must** be auditable, well-defined and justified against a demonstrable operational requirement. Vendor documentation describing requirements for Anti-Malware software scan exceptions **must** be indexed and archived for reference, auditing and review.	DE.CM-01 DE.CM-06
11.12.5	Anti-Malware software **must** be configured to log any malware detection incidents to a centralised repository that is actively reviewed.	DE.CM-01 DE.CM-06 PR.PS-04

Reference	Minimum Technical Security Measures	
11.12.6	Anti-Malware software **must** be configured to disinfect, delete, quarantine or encrypt malware upon detection. Encryption of the malware **must** be reversible in the case of false positive detection (i.e. an XOR of the file is generally sufficient).	DE.CM-01 DE.CM-06 PR.PS-05
11.12.7	Anti-Malware software **must** be configured to automatically update signature or definition files in near real-time from a centralised internal source and from the Internet directly as a fall-back mechanism.	ID.AM-08 PR.PS-02
11.12.8	Anti-Malware software **must** be running the latest version of the underlying detection engine as well as the signature or definition files.	ID.AM-08 PR.PS-02
11.12.9	Anti-Malware software procurement and deployment processes **must** consider the use of heuristic scanning methods as well as traditional signature or definition-based scanning. Consideration **must** also be given to the use of Next Generation products (including AI and machine learning capabilities), given that sophisticated malware is becoming more difficult for current signature-based products to detect.	DE.CM-01 DE.CM-06

Reference	Minimum Technical Security Measures	
11.12.10	Anti-Malware software **must** be periodically verified for integrity. Ideally this verification check **must** be managed via a centralised console and adequately monitored. The meaning of integrity is that the service/ process associated with the software is running, the software remains tamper proof, the file and folder scanning exceptions are as expected, the efficacy of the detection engine is reviewed, and the signature or definition files are being updated as expected.	DE.CM-09 ID.AM-08
11.12.11	Anti-Malware Software **must** have its resource management options appropriately configured to ensure that CPU, memory and hard disk usage are never exhausted during operation.	PR.IR-04

11.13. Content Inspection and Defence in Depth

(Important) this table contains ‘must’ activities

Reference	Minimum Technical Security Measures	
11.13.1	Any standard users **must** be subject to an allow listing and block listing URL reputation service for inspection for outbound Internet Browsing.	PR.AA-05 DE.CM-03 DE.CM-09
11.13.2	URL block listing reputational feeds for Internet Browsing **must** be updated in as near to real-time as operationally feasible on the Content Inspection boundary devices such as Next Generation Firewalls, Proxy Servers, or Web Content Filtering gateways referenced by the Internet Browsing boundary routers.	PR.PS-02 DE.CM-01

Reference	Minimum Technical Security Measures	
11.13.3	URL block listing and Content Inspection for Internet Browsing **must** work in a blocking state for known malicious sites. In other words, URL block listing Content Inspection **must not** work in an “Inspect only” state for known malicious sites.	PR.IR-02 DE.CM-01
11.13.4	Email Content Inspection **must** have a minimum two layers of Anti-Malware scan performed prior to persisting attachments to departmental resources. This will take the form of Email Content Inspection on the relevant Mail Gateway and on the desktop, server or mobile endpoints Anti-Malware software inspection engine.	PR.IR-02 DE.CM-01
11.13.5	Intrusion Prevention systems (IPS) **must** be configured and maintained with the latest signatures and rule sets to help mitigate malware intrusion attempts and Indicators of Compromise, including blocking outbound command-and-control traffic.	PR.PS-02 DE.CM-01
11.13.6	Content Inspection technology capable of operating in an active blocking mode, (rather than only inspecting content), **must** have a clear and tested set of procedures to overcome false positives that may affect legitimate business processing. Block mode **must** be set after the initial installation and learning phases are completed.	PR.IR-02 DE.CM-01

Reference	Minimum Technical Security Measures	
11.13.7	Wherever possible, complementary endpoint agent-based Defence in Depth technologies, e.g., Next Generation Anti-Malware Software (in addition to traditional Anti-Malware Software), host-based firewalls / intrusion prevention software and micro-virtualisation technologies **must** be utilised.	PR.IR-01 PR.IR-03
11.13.8	Consideration **must** be given to complementary agentless 'Defence in Depth' technologies such as Isolation and Rendering technologies, Sandboxing technologies (including API-based cloud sandboxing techniques) and Data Science based solutions to help identify Indicators of Compromise.	PR.IR-01 PR.IR-03
11.13.9	Consideration **must** be given to API-based email content detection and response capabilities, which can offer capabilities similar to email gateways, but are more dynamic and adaptive with the added advantage of continuous updates and integration with other security measures to provide a more comprehensive 'Defence in Depth' strategy. However it should be noted that these capabilities may be reliant on predefined indicators of compromise (IOCs) and may not be as effective against new or unknown threats.	DE.CM-09 DE.AE-03

11.14. Log Configuration and Collection

(Important) this table contains ‘must’ activities

Reference	Minimum Technical Security Measures	
11.14.1	Anti-Malware Software on every operational endpoint **must** be configured to log any disinfection, deletion, quarantine or encryption actions in near real-time to a centrally managed console for the Anti-Malware Software in use. Where near real-time logging is not possible, digest logging **must** be configured.	PR.PS-04
11.14.2	The Anti-Malware Centralised Console **must** be configured to forward in near real-time or in a digest format, logs aggregated from the clients it manages to a centralised SIEM system.	PR.PS-04
11.14.3	Any systems deployed for Content Inspection and Defence in Depth **must** have detection, inspection, blocking, quarantine, deletion, disinfection, traffic, and any encryption logs configured to forward to the centralised SIEM.	PR.PS-04 DE.CM-01 DE.CM-06
11.14.4	Configuration changes to operating parameters of any Anti-Malware technology including changes to logging facilities, administrative access, rule creation, and any content inspection updates **must** be tamper proof and logged either in near real-time or digested format to the centralised SIEM. This statement applies equally to system-initiated and system administrator changes to operating parameters including, exception modification, privilege access modifications and rule creation.	PR.AA-03 PR.PS-04 PR.IR-01
11.14.5	Separation of system administration duties **must** ensure that management of the centralised SIEM **does not** overlap with those privileged users supporting Malware protection services.	PR.AC-05

11.15. Log Review and Analysis

(Important) this table contains ‘must’ activities

Reference	Minimum Technical Security Measures	
11.15.1	Baseline Management Information of the Anti-Malware Software logs and the Defence in Depth system logs **must** be validated, reconciled and processed for monthly reporting. This process **must** include the removal of any false positives.	PR.PS-04 DE.AE-03
11.15.2	A quarterly review (more frequently if required) of trending data collected via Anti-Malware Software and Defence in Depth logs **must** be performed. The review **must** establish any trends in the threat landscape highlighting any monthly changes. This can both validate and act as a complementary data source for other threat intelligence sources.	PR.PS-04 DE.AE-03 ID.RA-03

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 2 – List of Security Outcomes Mapping

Ref	Security Outcome (Sub-category)	Related Security Measure
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	11.1.2
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	11.3.2, 11.9.6
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained Inventories of services provided by suppliers are maintained	11.1.3
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.3.1, 11.12.7, 11.12.8, 11.12.10
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	11.11.1

Ref	Security Outcome (Sub-category)	Related Security Measure
ID.RA-03	Internal and external threats to the organization are identified and recorded	11.11.1, 11.15.2
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	11.9.5
PR.AA-03	Users, services, and hardware are authenticated	11.7.1, 11.14.4
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.2.2, 11.2.3, 11.4.1, 11.4.2, 11.4.3, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.13.1
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	11.2.1
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.6.1, 11.6.2
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.7.1, 11.7.2

Ref	Security Outcome (Sub-category)	Related Security Measure
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.5, 11.3.1, 11.3.2, 11.9.3, 11.9.4, 11.12.7, 11.12.8, 11.13.2, 11.13.5
PR.PS-04	Log records are generated and made available for continuous monitoring	11.4.3, 11.12.5, 11.14.1, 11.14.2, 11.14.3, 11.14.4, 11.15.1, 11.15.2
PR.PS-05	Installation and execution of unauthorized software are prevented	11.5.5, 11.8.1, 11.9.1, 11.9.2, 11.10.3, 11.12.6
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	11.3.2, 11.4.1, 11.4.2, 11.8.2, 11.13.7, 11.13.8, 11.14.4
PR.IR-02	The organization's technology assets are protected from environmental threats	11.13.3, 11.13.4, 11.13.6
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	11.13.7, 11.13.8
PR.IR-04	Adequate resource capacity to ensure availability is maintained	11.12.11
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.1.4, 11.1.5, 11.10.1, 11.10.2, 11.12.1, 11.12.2, 11.12.3, 11.12.4, 11.12.5, 11.12.6, 11.12.9, 11.13.2, 11.13.3, 11.13.4, 11.13.5, 11.13.6, 11.14.3

Ref	Security Outcome (Sub-category)	Related Security Measure
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.13.1
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	11.10.2, 11.12.1, 11.12.2, 11.12.3, 11.12.4, 11.12.5, 11.12.6, 11.12.9, 11.14.3
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.1.5, 11.12.10, 11.13.1, 11.13.9
DE.AE-03	Information is correlated from multiple sources	11.15.1, 11.15.2, 11.13.9
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	11.11.1

Appendix B – Internal references

Below is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal references

Ref	Document	Publicly Available*
A	SS-010 Desktop Operating System Security Standard	Yes
B	SS-033 Security Patching Standard	Yes
C	SS-001 pt.2 Privileged User Access Security Standard	Yes
D	Security Assurance Strategy	No
E	SS-014 Security Incident Management Standard	Yes

*Requests to access non-publicly available documents **should** be made to the Authority Contracts/Supplier Manager.

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 4 – External references

External Documents List
NIST Cyber Security Framework
CIS Critical Security Controls set
OWASP Open Web Application Security Project
NCSC - Mitigating malware and ransomware attacks

Appendix D – Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
CMDB	Configuration Management Database	Industry term
CVE	Common Vulnerabilities and Exposures	Industry term
DWP	Department for Work and Pensions.	UK Government
GSCP	Government Security Classification Policy	UK Government
HID	Human Interface Devices	Industry term
IDS	Intrusion Detection System	Industry term
iFrames	Inline Frames	Industry term
IPS	Intrusion Prevention System	Industry term
ISO	International Organization for Standardization	Industry term
MAC	Mandatory Access Control	Industry term
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OS	Operating System	Industry term
OWASP	Open Web Application Security Project	Open source

Abbreviation	Definition	Owner
OWASP ASVS	(OWASP) Application Security Verification Standard	Open source
RDP	Remote Desktop Protocol	Industry term
SIEM	Security Incident Event Management	Industry term
SLA	Service Level Agreement	Industry term
SSH	Secure Shell	Industry term
VPN	Virtual Private Network	Industry term

Appendix E – Glossary

Table 6 – Glossary

Term	Definition

Appendix F – Accessibility artefacts

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

DWP Digital Accessibility Policy | DWP Intranet

DWP Accessibility Manual

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies