Security Standard – Protective Monitoring (SS-012)

Chief Security Office

Date: 11/10/2022

Department for Work & Pensions

This Protective Monitoring 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 technical security controls. For the purposes of this standard, the term DWP and Authority 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. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	29/05/2018
2.0		Full update in line with current best practices and standards, includes NIST references and describes outcomes. • Updated introduction, audience, purpose, scope and exceptions • Described the relationship and exceptions with Business Audit, Physical Security Standards, Fraud and SaaS cloud • Replaced use of technical control requirements with minimum security measures • Reformatted document, using 3 headings that describe minimum security measures • Added NIST subcategory references against each security measure • Added Appendix A describing security outcomes mapped to relevant security measures and NIST subcategories • Updated all references and links to publications • DPA and ICO log requirements applied • Added a statement explaining responsibility for	11/10/2022

		implementing controls and conditions for ITHC / security test. • Scope and 11.3.5 updated for log storage responsibility.	

3. Approval history

Version	Approver	Role	Date
1.0		Chief Security Officer	29/05/2018
2.0		Chief Security Officer	11/10/2022

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

4. Compliance

Security Assurance teams will verify compliance with this Standard through various methods, including but not limited to, internal and external audits, and feed back to the appropriate Authority Risk and System Owner.

5. Exception Process

In this document the term **“must”** in bold letters is used 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 measure’s details 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 limited to, solution architects, security architects, domain architects, engineers, developers, security teams, security monitoring teams, project teams, including suppliers engaged in the design, development, and the implementation of Information and Communications Technology (ICT) systems.

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

To ensure new and existing Authority ICT systems are appropriately monitored for suspicious, or potential comprises, the minimum technical security measures defined in this standard **must** be implemented across the Authority ICT estate. For the avoidance of doubt, the Authority ICT estate includes environments provisioned in the cloud. There are however some exceptions to this which are set out in Section 10.

While security monitoring is central to the identification and detection of threats to Authority ICT systems, it relies on proportionate, reliable logging and device management practices to be fully effective. As such, this standard aims to cover the end-to-end process for security log management.

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. [See Appendix C for external references].

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 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 protective monitoring controls are implemented consistently across the Authority ICT estate and supplier base.
- ensure logging and monitoring activities are proportionate to the context of the system in question, taking into consideration the threats faced by the Authority.
- ensure the confidentiality, integrity, and availability of security log data.
- ensure Authority ICT systems and those managed by third party suppliers and partners, are appropriately monitored for potential compromises or suspicious activity.
- introduce an additional layer of defence in depth to Authority ICT systems.
- assist with internal investigations into malpractice.

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. The outcomes are based on the official NIST subcategories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and they can be found in Appendix A of every standard.

9. Purpose

The purpose of this standard is to ensure the Authority and relevant suppliers are able to detect and respond to potential cyber-attacks quickly, so that any adverse impacts on key operational systems and end users are minimised.

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

All Authority ICT systems whether hosted on premise or in the cloud, including those managed by third parties and suppliers are in scope of this standard. The only exception being SaaS offerings which is covered in SS-023 Cloud Computing Security Standard [Ref. A].

This standard only covers security log analysis. Appropriate log copies are taken from source systems for the purpose of performing monitoring and analysis, e.g., as part of an investigation.

This standard does not cover logging and monitoring of physical security controls that are technical in nature deployed at Authority premises e.g. door access control systems.

The logging and monitoring of business users and applications, including the actions of self-service customers, for the purposes of fraud and error detection is also not covered by this standard.

Lastly, device management while critical to effective security logging and monitoring, is outside the scope of this standard and is covered elsewhere.

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 with regards to security log management, so that the security outcomes described in Appendix A can be achieved. For ease of reference, the relevant 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.

Furthermore, the security measures have been divided into three sections to help users navigate more easily to the security measures that are likely to be relevant to them. However, the entire standard **should** be read for completeness. The sections are as follow:

- **Section 1**. Protective Monitoring Posture applies to all users.
- **Section 2**. Requirements for ICT systems is applicable to anyone designing a solution.
- **Section 3**. Central Monitoring Requirements is applicable to security monitoring teams. Note. This is not exclusively aimed at security monitoring teams.

Section 1. Protective Monitoring Posture

11.1 General Security Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	All ICT systems (including cloud-based deployments) **must** conform to the Authority Protective Monitoring Security Policy [Ref. D] requirements detailing what needs to be secured and why.	PR.PT-1
11.1.2	All ICT systems **must** be hardened using applicable Authority Security Standards and vendor security guidelines where available. Authority Security Standards **must** take precedence over vendor security guidelines.	PR.PT-3

11.1.3	Once auditing and logging has been configured on a given ICT system, formal testing **must** be carried out to verify events are being locally logged, forwarded and received by the Authority as expected. This process **must** be repeated following any significant changes made to the ICT system.	DE.DP-3, PR.IP-3
11.1.4	Log data ownership **must** be recorded in an Information Asset Inventory or other record of organisational assets.	PR.PT-1
11.1.5	System Owners **must** classify log data in accordance with the Government Classification Scheme (Appendix C), taking into consideration aggregation and association factors.	PR.PT-1, ID.AM-5
11.1.6	All users **must** be prohibited from accessing or modifying their own logs.	PR.PT-1, DE.CM-3
11.1.7	Access to log data **must** be read-only. All log review activities **must** be recorded for audit purposes.	PR.AC-4, PR.IP-3
11.1.8	Separation of duties must be maintained between privileged users and auditors' roles in accordance with SS-001 (part 2) Privileged User Access Security Standard [Ref. E].	PR.AC-4
11.1.9	Users **must** be prevented from disabling logging. It is acknowledged that Privileged Users will legitimately adjust logging levels under authorised and controlled circumstances and their Privileged actions will be logged accordingly.	PR.AC-4

Section 2. Requirements for ICT systems

11.2 Local Log generation

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	All ICT systems **must** be configured to generate log events. The logging and auditing configuration implemented **must** also be documented and agreed with the Authority.	PR.PT-1, DE.DP-2
11.2.2	All systems in scope **must** be synchronised to the Authority Reference (Master) Clock so that its timestamp matches to those generated by other systems. NTP protocol **must** be used to synchronise log source time with the Authority Master Clock. For cloud based systems, the cloud providers' time services are sufficient for time reference synchronisation.	PR.DS-6 PR.PT-1 DE.AE-3 DE.DP-2
11.2.3	System time **must** be accurate to within the agreed time of the Reference Clock. The error margin of time accuracy **must** be according to the business requirements.	PR.DS-6 PR.PT-1 DE.AE-3 DE.DP-2
11.2.4	The following information **must** be logged where available: - Timestamp. - Description of the log or event. - Severity level (e.g., High, Medium, Low) - Hostname. - IP Address.	PR.PT-1

	- Username (e.g., UPN, SAM Account)	
11.2.5	Audit logs relating to user actions **must** contain sufficient information to uniquely technically identify the user to which they pertain. Accordingly, logging processes **must** minimise the capture of personal data. Logs containing personal data, e.g., some IP addresses, must be subject to DPIA and protected in accordance with current DPA and GDPR legislation.	PR.PT-1, DE.AE-3
11.2.6	System owners **must** define and agree with the Authority the required log data types for log sources, using the information in 11.2.4 above as a baseline and in line with the Authority's Protective Monitoring Policy. System owners **must** also record this information in the system design document.	PR.PT-1
11.2.7	System owners **must** identify the event types and attributes of their environment. Event types **must** be agreed with the Authority. System owner **must** document event types in the design document.	PR.PT-1
11.2.8	All privileged user activities on any ICT system **must** be logged.	PR.PT-1, DE.CM-3
11.2.9	All Logs **must** be immutable i.e., protected against: • deletion and tampering • unauthorised access • The deletion and modification of logs **must** be logged • The record of deleted logs **must not** contain a copy of the log	PR.DS-1, PR.DS-5, PR.AC-4 DE.CM-3

11.3 Local Log Transmission

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Where there is a need to convert logs with different content and format to a single standard format, the standard format **must** be agreed with the Authority, so it matches the format used by the centralised monitoring tool.	PR.PT-1
11.3.2	The transmission of log messages **must** be secured in accordance with the SS-006 Security Boundaries Security Standard [Ref. F].	PR.DS-2, PR.PT-4
11.3.3	When using log aggregation points, log integrity **must** be maintained when forwarding log data to an Authority approved centralised monitoring system.	PR.DS-6, DE.AE-3
11.3.4	Where supported, logs **must** be digitally signed and transmitted to an Authority approved centralised monitoring system. This **must** be accomplished in compliance with SS-007 Use of Cryptography Security Standard [Ref. G] and SS-002 PKI & Key Management Security Standard [Ref. H].	PR.DS-6
11.3.5	Logs **must** be forwarded to an Authority approved centralised monitoring system close to real-time as possible (no more than 10 minutes, less than 1 minute is expected) e.g., for operational purposes or criminal investigation. Retention of log data	PR.PT-1, DE.AE-3

	must comply with the Authority's Information Management Policy [Ref. I].	
11.3.6	Where supported, performance alerts generated by ICT Systems **must** be forwarded to an Authority approved centralised monitoring system.	DE.CM-1, DE.AE-3

Section 3. Central Monitoring Requirements

11.4 Central Log Storage

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Log data **must** be retained in accordance with the Authority's Information Management Policy [Ref. I].	PR.PT-1
11.4.2	Log data **must** be preserved beyond the normal retention period if used for investigation purposes. If a retained log contains Personal Information, the DPA / GDPR control requirements current at the point of deletion are inherited and **must** be implemented.	PR.PT-1
11.4.3	All logs **must** have as a minimum the same level of protection as the system and data from which they originate.	ID.AM-5
11.4.4	Where log data is retained by third parties, the contracting party **must** define and agree an appropriate access policy with the Authority. The access policy **must** be referenced in the design document.	PR.AC-4, PR.PT-1

11.4.5	Stored logs **must** be immutable i.e., protected against: • deletion and tampering • unauthorised access	PR.AC-4, PR.AC-2, PR.DS-1
11.4.6	The integrity of log data **must** be verified and preserved.	PR.DS-1
11.4.7	Backups of log data **must** be managed in compliance with SS-035 Secure Backup and Restore Security Standard [Ref. J].	PR.IP-4
11.4.8	Backups of log data **must** be tested regularly in accordance with the SS-035 Secure Backup and Restore Security Standard [Ref. J]. to ensure log data is still readable and in correct format.	PR.IP-4
11.4.9	Offline log backups including archived log data **must** be stored in an Authority Approved storage service that provides the capability of being restored in a timely manner, (as per 11.4.7 above) this **must** be agreed with the system owner.	PR.IP-4, PR.IP-9, PR.PT-1

11.5 Central Log Analysis

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	All logs mandated by this or other Authority technical security standards **must** be monitored taking into consideration the criticality of the system and the severity level of the event being audited. Frequency and processes **must** be documented and agreed with the Authority.	DE.CM-2, RS.AN-1, DE.CM-1, DE.CM-3, DE.DP-2

11.5.2	Log data **must** be reviewed regularly based on the criticality of the system and the severity level of the event being audited.	DE.AE-2, DE.DP-4
11.5.3	Deletion, disabling or modification of logs **must** be monitored and alerted in as near real time as possible.	DE.CM-3
11.5.4	Integrity of log data **must** be monitored and alerted on if any corruption occurs close to real-time as possible. A record of the corrupted version **should** be stored separate to the corrected log so that a record is maintained for reference, but the erroneous log is not accessible in live.	RS.AN-1 PR.PT1
11.5.5	Any log incident investigation **must** follow the requirements set out in the Security Incident Management Policy [Ref. K].	PR.IP-9

11.6 Central Log Disposal

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Log data **must** be disposed of in accordance with the Authority’s security classification policy [Ref. L] and SS-036: Secure Sanitisation and Destruction Security Standard [Ref. M].	PR.IP-6

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 measures
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	11.1.5, 11.4.3
PR.AC-2	Physical access to assets is managed and protected	11.4.5
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.7, 11.1.8, 11.1.9, 11.2.9, 11.4.4, 11.4.5
PR.DS-1	Data-at-rest is protected	11.2.9, 11.4.5, 11.4.6
PR.DS-2	Data-in-transit is protected	11.3.2
PR.DS-5	Protections against data leaks are implemented	11.2.9
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.3.3, 11.3.4

PR.IP-3	Configuration change control processes are in place	11.1.3, 11.1.7
PR.IP-4	Backups of information are conducted, maintained, and tested	11.4.7, 11.4.8, 11.4.9
PR.IP-6	Data is destroyed according to policy	11.6.1
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.4.9, 11.5.5
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.1.1, 11.1.4, 11.1.5, 11.1.6, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.3.1, 11.3.5, 11.4.1, 11.4.2, 11.4.4, 11.4.9
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.1.2
PR.PT-4	Communications and control networks are protected	11.3.2
DE.AE-2	Detected events are analysed to understand attack targets and methods	11.5.2
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.2.5, 11.3.3, 11.3.5, 11.3.6

DE.CM-1	The network is monitored to detect potential cybersecurity events	11.3.6, 11.5.1
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	11.5.1
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	11.1.6, 11.2.8, 11.2.10, 11.5.1, 11.5.3
DE.DP-2	Detection activities comply with all applicable requirements	11.1.10, 11.2.1, 11.5.1
DE.DP-3	Detection processes are tested	11.1.3
DE.DP-4	Event detection information is communicated	11.5.2
RS.AN-1	Notifications from detection systems are investigated	11.5.1, 11.5.4

Appendix B. Internal references

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

Table 3 – Internal References

Ref	Document	Publicly Available
A	SS-023 Cloud Computing Security Standard	Y
B	SS-034 Business Audit Security Standard	N
C	SS-027 Application Security Testing Security Standard	N
D	DWP Protective Monitoring Security Policy	Y
E	SS-001 (part 2): Privileged User Access Security Standard	Y
F	SS-006 Security Boundaries Security Standard	Y
G	SS-007 Use of Cryptography Security Standard	Y
H	SS-002 PKI & Key Management Security Standard	Y
I	Information Management Policy	Y
J	SS-035 Security Standard: Secure backup and restore	Y
K	Security Incident Management Policy	TBC
L	DWP Security Classification Policy	Y
M	SS-036 Security Standard: Sanitisation and Destruction	Y

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
CIS Critical Security Controls v8 controls set
NIST SP 800-92 - Guide to Computer Security Log Management, September 2006
NIST SP 800-137 - Information Security Continuous Monitoring (ISCM), September 2011
CESG Good Practice Guide No. 13 - Protective Monitoring for HMG ICT Systems, October 2012
Government Classification Scheme
NCSC 10 steps to Cyber Security – Logging and Monitoring
NCSC Device Security Guidance – Logging and Protective Monitoring
Logging | ICO

Appendix D. Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
DDA	Digital Design Authority	Internal body
GSCS	Government Security Classification Scheme	UK Government
HMG	Her Majesty's Government	UK Government
ICT	Information and Communications Technology	Industry term

Abbreviation	Definition	Owner
ISO	International Organization for Standardization	Industry term
NCSC	National Cyber Security Centre	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OWASP	Open Web Application Security Project	Global
PDU	Product Delivery Units	Internal term
PII	Personally, Identifiable Information	Industry term
UTC	Coordinated Universal Time	Industry term

Appendix E. Glossary

Table 6 – Glossary

Term	Definition
Alert	An event/message generated when certain triggers or thresholds or conditions or rules are met. An alert is a prioritise event. Similarly, it is a message raised by a business process that indicates the high probability of an information security incident requiring investigation.
Analysis	This is the process of analysing the recorded security monitoring events or log data in order to determine suspicious events, detect compromise, security breaches or policy noncompliance. Analysis encompasses a number of techniques aimed at thoroughly examining log data, such as correlation, filtering, querying, business rules and trending.

Audit	The systematic, independent and documented process for obtaining audit evident and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
Business Audit	The Authority's terminology for audit trail of business systems data, audit trail data storage (archive) and for making audit data available for interrogation or investigative purposes. That is, DWP Business Audit is the technology and processes to monitor events and transactions generated and viewed by business users of ICT systems, with access to customer data, to detect and highlight misuse and potential fraud.
End-to-end Testing	Documented verification of what has been sent has been received.
Event	A message produces by a business process or system when a set of activities occur.
ICT Systems	Information and Communications Technology - Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).
Incident	A potential or actual breach or violation of security policy or business process or set of business objectives.
Incident Management	The process aimed at minimising immediate impact and long-term business impact of incidents and to prevent re-occurrences.
Log Management	The process for generating, transmitting, storing, analysing, and disposing of log data.
Log Normalization	Converting each log data field to a particular data representation and categorizing it consistently.

Logging	The process of collecting and storing logs (audit logs, event logs, system logs, application or database logs) for the purpose of analysing it to detect abnormal or suspicious activity or violation of policy.
Monitoring	Assessing information contained in logs in real or near-real time to identify anomalies, patterns, or events of interest.
Network Management System	A set of hardware and software which are used to monitor, inspect and manage individual components within a network.
OFFICIAL	Information classification mark, identified in the Government Security Classification Policy.
Privileged User	A Privileged User is a user who has an elevated level of access to a network, computer hardware or system components or functionality and is authorised to perform functions that standard and elevated users are not authorised to perform.
System Owners	Individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of the information system in question.

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