
Security Standard – Protective Monitoring (SS-012)

Chief Security Office

Date: 18/09/2024



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 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. Table of Contents

| | | |
|--|-------------------------------------|----|
| 1. | Table of Contents | 3 |
| 2. | Revision history | 4 |
| 3. | Approval history | 6 |
| 4. | Compliance | 6 |
| 5. | Exception Process | 6 |
| 6. | Audience | 7 |
| 7. | Accessibility statement | 7 |
| 8. | Introduction | 7 |
| 9. | Purpose | 8 |
| 10. | Scope | 9 |
| 11. | Minimum Technical Security Measures | 10 |
| Section 1. Protective Monitoring Posture | | 11 |
| 11.1 | General Security Requirements..... | 11 |
| Section 2. Requirements for ICT systems | | 12 |
| 11.2 | Local Log generation | 12 |
| 11.3 | Local Log Transmission..... | 14 |
| Section 3. Central Monitoring Requirements | | 15 |
| 11.4 | Central Log Storage..... | 15 |
| 11.5 | Central Log Analysis..... | 17 |
| 11.6 | Central Log Disposal | 18 |
| 12 Appendices | | 19 |
| Appendix A. | Security Outcomes | 19 |
| Appendix B. | Internal references | 22 |
| Appendix C. | External references | 23 |
| Appendix D. | Abbreviations | 23 |
| Appendix E. | Glossary | 24 |
| Appendix F. | Accessibility artefacts | 26 |

2. Revision history

| Version | Author | Description | Date |
|---------|--------|---|------------|
| 1.0 | | First published version | 29/05/2018 |
| 2.0 | | <p>Full update in line with current best practices and standards, includes NIST references and describes outcomes.</p> <ul style="list-style-type: none"> • 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 implementing | 11/10/2022 |

| | | | |
|-----|--|--|------------|
| | | <p>controls and conditions for ITHC / security test.</p> <ul style="list-style-type: none"> • Scope and 11.3.5 updated for log storage responsibility. | |
| 2.1 | | <p>All NIST references reviewed and updated to reflect NIST 2.0</p> <p>All security measures reviewed in line with risk and threat assessments</p> <p>11.1.2 Reference added for Malware Protection standard</p> <p>11.1.4 Log ownership</p> <p>11.1.5 Sensitive data and PII</p> <p>11.1.10 Monitoring for failed log collection, disabling, tampering or redirection</p> <p>11.2.4 Event Codes</p> <p>11.2.5 Automated actions</p> <p>11.2.9, 11.4.5, 11.4.6</p> <p>References added for encryption and PKI standards</p> <p>11.3.4 Sign logs as soon as created</p> <p>11.5.2 Behavioural analysis</p> <p>11.5.3 Unauthorised redirection</p> | 18/09/2024 |

3. Approval history

| Version | Approver | Role | Date |
|---------|----------|------------------------|------------|
| 1.0 | | Chief Security Officer | 29/05/2018 |
| 2.0 | | Chief Security Officer | 11/10/2022 |
| 2.1 | | Chief Security Officer | 18/09/2024 |

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. [See Security Assurance Strategy – Ref. O].
- independent external audit

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

5. Exception 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 measures 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 limited to, solution architects, security architects, domain architects, technical engineers, developers, security teams, security monitoring 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

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 Authority or our third party providers, such as the CIS Critical Security 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 sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF) and they can be found in Appendix A of every standard.

Responsibility for implementation of technical protective monitoring controls rests with the Protective Monitoring Service System Owner and with the Consuming service systems owners. Accordingly, this standard supports those responsible parties.

9. Purpose

The purpose of this standard is to ensure that 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], where additional measures may be required from the Cloud Service Provider who has some contractual responsibility for protective monitoring.

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. This is addressed in SS-034 Business Audit Security Standard [Ref. B] and should be read in conjunction with this standard where appropriate.

The frequency and conditions requiring both an ITHC and security testing, i.e., at go-live and when system changes occur are addressed in SS-027 Security Testing Standard [Ref. C] which should be read in conjunction with this standard as appropriate.

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 DWP Protective Monitoring Security Policy [Ref. D] requirements detailing what needs to be secured and why. | PR.PS-04 DE.CM-01 |
| 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, in particular SS-015 Malware Protection Security Standard [Ref. N]. | PR.DS-01 PR.DS-02 |
| 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 Security Monitoring team as expected. This process must be repeated following any significant changes made to the ICT system. | PR.PS-04 |
| 11.1.4 | Log data ownership must be recorded in an Information Asset Inventory or other record of organisational assets. Its important to note that the system or business owner retains ownership of logs until they are archived or deleted within the Authority. | PR.PS-04 ID.AM-07 |
| 11.1.5 | System Owners must classify log data in accordance with the Government Classification Scheme (Appendix C), taking into consideration sensitive data, Personally Identifiable Information, aggregation and association factors. | PR.PS-04 ID.AM-05 |
| 11.1.6 | All users must be prohibited from accessing or modifying their own logs. | PR.PS-04 PR.AA-03 PR.AA-05 |

| | | |
|---------|--|----------------------|
| 11.1.7 | Access to log data must be read-only. All log review activities must be recorded for audit purposes. | PR.AA-05 PR.PS-04 |
| 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.AA-05 |
| 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.AA-05 |
| 11.1.10 | Monitoring and alerting must be in place to identify failed log collection, where logging has been disabled, or where there is evidence of tampering or log redirection. | PR.PS-04 |

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 Security Monitoring team. | PR.PS-04 |
| 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, as the Authority does not have reliable means to share Master Clock data with external parties. | PR.DS-01 PR.DS-02 DE.AE-03 |

| | | |
|--------|---|----------------------------------|
| 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-01 PR.DS-02 DE.AE-03 |
| 11.2.4 | The following information must be logged where available: <ul style="list-style-type: none"> • Timestamp. • Description of the log or event. • Severity level (e.g., High, Medium, Low) • Hostname. • IP Address. • Username (e.g., UPN, SAM Account) • Event codes or other unique identifiers | PR.PS-04 |
| 11.2.5 | Audit logs relating to user actions (including those due to automated actions e.g. robotic process automation) 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.PS-04 PR.DS.01 |
| 11.2.6 | System owners must define and agree with the Security Monitoring team the required log data types for log sources, using the information in 11.2.4 above as a baseline and in line with the DWP Protective Monitoring Policy. System owners must also record this information in the system design document. | PR.PS-04 ID.AM-02 |
| 11.2.7 | System owners must identify the event types and attributes of their environment. Event types must be agreed with the Security Monitoring team. System owner must document event types in the design document. | PR.PS-04 ID.AM-02 |
| 11.2.8 | All privileged user activities on any ICT system must be logged. | PR.PS-04 DE.CM-03 |

| | | |
|--------|--|--|
| 11.2.9 | <p>All Logs must be immutable i.e., protected against:</p> <ul style="list-style-type: none"> • 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 <p>See SS-007 Use of Cryptography [Ref. G] and SS-002 PKI & Key Management [Ref. H] Security Standards for further information.</p> | PR.DS-01 PR.DS-02 PR.DS-10 DE.CM-03 |
|--------|--|--|

11.3 Local Log Transmission

| Reference | Minimum Technical Security Measures | NIST ID |
|-----------|--|----------------------------------|
| 11.3.1 | <p>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 Security Monitoring team, so it matches the format used by the centralised monitoring tool.</p> | PR.PS-04 |
| 11.3.2 | <p>The transmission of log messages must be secured in accordance with the SS-006 Security Boundaries Security Standard [Ref. F] or follow a DWP Security Monitoring Pattern where available.</p> | PR.DS-02 PR.IR-01 |
| 11.3.3 | <p>When using log aggregation points, log integrity must be maintained when forwarding log data to an Authority approved centralised monitoring system.</p> | PR.PS-04 PR.DS-02 DE.AE-03 |
| 11.3.4 | <p>Where supported, logs must be digitally signed as soon as they are created 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].</p> | PR.DS-02 |

| | | |
|--------|---|----------------------------------|
| 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 must comply with the DWP Information Management Policy [Ref. I]. | PR.PS-04 DE.AE-03 |
| 11.3.6 | Where supported, performance alerts generated by ICT Systems must be forwarded to an Authority approved centralised monitoring system. | DE.AE-03 PR.PS-04 DE.CM-09 |

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 Information Management Policy [Ref. I]. | PR.PS-04 |
| 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.PS-04 ID.AM-08 |
| 11.4.3 | All logs must have as a minimum the same level of protection as the system and data from which they originate. | PR.DS-01 |
| 11.4.4 | Where log data is retained by third parties, the contracting party must define and agree an appropriate access policy with the assigned Security Architect or Contract Manager. The access policy must be referenced in the design document. | PR.AA-05 GV.PO-01 |

| | | |
|--------|--|---------------------------------|
| 11.4.5 | <p>Stored logs must be immutable i.e., protected against:</p> <ul style="list-style-type: none"> • deletion and tampering • unauthorised access <p>See SS-007 Use of Cryptography [Ref. G] and SS-002 PKI & Key Management [Ref. H] Security Standards for further information.</p> | <p>PR.AA-05</p> <p>PR.DS-01</p> |
| 11.4.6 | <p>The integrity of log data must be verified and preserved.</p> <p>See SS-007 Use of Cryptography [Ref. G] and SS-002 PKI & Key Management [Ref. H] Security Standards for further information.</p> | <p>PR.DS-01</p> |
| 11.4.7 | <p>Backups of log data must be managed in compliance with SS-035 Secure Backup and Recovery Security Standard [Ref. J].</p> | <p>PR.DS-11</p> |
| 11.4.8 | <p>Backups of log data must be tested regularly in accordance with the SS-035 Secure Backup and Recovery Security Standard [Ref. J]. to ensure log data is still readable and in correct format.</p> | <p>PR.DS-11</p> |
| 11.4.9 | <p>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.</p> | <p>PR.DS-11</p> <p>PR.DS-01</p> |

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 Security Monitoring team. | PR.PS-04 DE.CM-01 |
| 11.5.2 | Log data must be reviewed regularly (including the use of behavioural analysis where appropriate) based on the criticality of the system and the severity level of the event being audited. | ID.AM-05 DE.AE-04 |
| 11.5.3 | Deletion, disabling, modification, or unauthorised redirection of logs must be monitored and alerted in as near real time as possible. | DE.CM-09 |
| 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. | DE.CM-09 |
| 11.5.5 | Any log incident investigation must follow the requirements set out in the Security Incident Management Standard [Ref. K]. | ID.IM-04 |

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]. | ID.AM-08 |

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.PO-01 | Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced | 11.4.4 |
| ID.AM-02 | Inventories of software, services, and systems managed by the organization are maintained | 11.2.6, 11.2.7 |
| ID.AM-05 | Assets are prioritized based on classification, criticality, resources, and impact on the mission | 11.1.5, 11.5.2 |
| ID.AM-07 | Inventories of data and corresponding metadata for designated data types are maintained | 11.1.4 |
| ID.AM-08 | Systems, hardware, software, services, and data are managed throughout their life cycles | 11.4.2, 11.6.1 |
| ID.IM-04 | Incident response plans and other cybersecurity plans that affect | 11.5.5 |

| | | |
|----------|---|--|
| | operations are established, communicated, maintained, and improved | |
| PR.AA-03 | Users, services, and hardware are authenticated | 11.1.6 |
| 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 | 11.1.6, 11.1.7, 11.1.8, 11.1.9, 11.4.4, 11.4.5 |
| PR.DS-01 | The confidentiality, integrity, and availability of data-at-rest are protected | 11.1.2, 11.2.2, 11.2.3, 11.2.9, 11.4.3, 11.4.5, 11.4.6, 11.4.9 |
| PR.DS-02 | The confidentiality, integrity, and availability of data-in-transit are protected | 11.1.2, 11.2.2, 11.2.3, 11.2.9, 11.3.2, 11.3.3, 11.3.4 |
| PR.DS-10 | The confidentiality, integrity, and availability of data-in-use are protected | 11.2.9 |
| PR.DS-11 | Backups of data are created, protected, maintained, and tested | 11.4.7, 11.4.8, 11.4.9 |
| PR.PS-04 | Log records are generated and made available for continuous monitoring | 11.1.1, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.1.10, 11.2.1, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.3.1, 11.3.3, 11.3.5, 11.3.6, 11.4.1, 11.4.2, 11.5.1, |
| PR.IR-01 | Networks and environments are protected from unauthorized logical access and usage | 11.3.2 |

| | | |
|----------|--|--|
| DE.CM-01 | Networks and network services are monitored to find potentially adverse events | 11.1.1, 11.5.1 |
| DE.CM-03 | Personnel activity and technology usage are monitored to find potentially adverse events | 11.2.8, 11.2.9 |
| DE.CM-09 | Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events | 11.3.6, 11.5.3, 11.5.4 |
| DE.AE-03 | Information is correlated from multiple sources | 11.2.2, 11.2.3, 11.3.3, 11.3.5, 11.3.6 |
| DE.AE-04 | The estimated impact and scope of adverse events are understood | 11.5.2 |

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 Security Testing 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 Backup & Recovery Security Standard | Y |
| K | Security Incident Management Policy | TBC |
| L | DWP Security Classification Policy | Y |
| M | SS-036 Sanitisation and Destruction Security Standard | Y |
| N | SS-015 Malware Protection Security Standard | Y |
| O | DWP Security Assurance Strategy | N |

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 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 |
| ISO | International Organization for Standardization | Industry term |

| Abbreviation | Definition | Owner |
|--------------|---|---------------|
| 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, Authority 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:

DWP Digital Accessibility Policy | DWP Intranet

<https://accessibility-manual.dwp.gov.uk/>

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

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