Protective Monitoring Standard: For External Use (SS-012)

Chief Security Office

Date: 29/05/18

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

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

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

1. Contents

2. Introduction

2.1. This Protective Monitoring Standard provides the list of requirements that are necessary to effectively monitor operational systems, in order to identify potential compromises or suspicious activity occurring on those systems.

2.2. The security controls presented in this standard are taken from examples of international best practice for protective monitoring and have been tailored for Departmental suitability.

3. Purpose

3.1. The purpose of this document is to enable external suppliers and bidders teams to work to a defined set of security requirements which enable protective monitoring solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for logging and monitoring. More detailed information will be available under certain circumstances.

3.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

4. Exceptions

4.1. In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

4.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to Design Authority (DA) where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

4.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

4.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

5. Audience

5.1. This standard is intended for external suppliers and bidders who are provisioning ICT systems for departmental use.

6. Scope

6.1. The security controls presented in this document are applicable to all ICT system deployments within the DWP. This includes deployments in external or cloud hosting providers.

6.2. The security control requirements laid out in this standard are product agnostic and applicable for all information systems that are provisioned for departmental use.

6.3. This standard covers logging, monitoring, and alerting of technical security events, also known as Security Information Event Management. Business and financial audit (for fraud and error detection purposes) is covered elsewhere, in Security Standard – Business Audit.

7. Security Controls Assurance

7.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

8. Technical Security Control Requirements

8.1. Protective Monitoring Posture

Reference	Security Control Requirement
8.1.1.	All ICT systems MUST conform to the Security Policy requirements detailing what needs to be secured and why.
8.1.2.	Protective Monitoring policy document MUST detail what events are to be logged on each component of that system, in compliance with both requirements in the relevant security standard for that system and the general requirements detailed in this document.
8.1.3.	A baseline level of Protective Monitoring Controls MUST be established.
8.1.4.	A risk assessment MUST be carried out to determine additional controls if the baseline controls does not fully address or mitigate risks.
8.1.5.	Periodic end-to-end testing MUST be conducted to assure that all events that needs to be logged are actually captured in the logs.
8.1.6.	The log set up MUST be discussed with the appropriate project team.
8.1.7.	The ownership of the log data MUST be clearly defined.

8.1.8.	Log data MUST be classified at the appropriate level of the system and data intended to be protected.

8.2. Log Naming Conventions

Reference	Security Control Requirement
8.2.1.	All audit and system logs MUST follow the departmental logging naming conventions which should be clear and efficient.

8.3. Log Field Requirements

Reference	Security Control Requirement
8.3.1.	System clock MUST be synchronised to the DWP time source so that its timestamp matches to those generated by other systems. In an exception case, where devices does not support clock synchronisation manual maintenance and a process MUST be provided and agreed with the project team.
8.3.2.	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.
8.3.3.	All logs MUST record date and time in a consistent and agreed format. UTC is the required time zone.
8.3.4.	All audit logs MUST contain timestamp.
8.3.5.	All ICT system in scope MUST be configured to generate appropriate log events.
8.3.6.	All ICT system in scope MUST be configured to generate heartbeat events.
8.3.7.	Logs MUST include hostname and IP addresses
8.3.8.	Where log data contain PII, appropriate privacy measures MUST be taken to protect those logs. If required, sensitive information MUST be masked, tokenised or encrypted.
8.3.9.	Any logs relating to user actions MUST contain enough information to uniquely identify the user to which they pertain.
8.3.10.	Log aggregation points MUST include a cryptographic checksum, which complies with Security Standard: Use of Cryptography.
8.3.11.	Where logs are digitally signed, this MUST be accomplished in compliance with Security Standard: Use of Cryptography.
8.3.12.	Logs messages MUST be stored in the agreed simple standard format. Syslog message format is recommended.
8.3.13.	Log messages MUST be sent and received securely over the network.

8.4. Event Requirements

Reference	Security Control Requirement
8.4.1.	System configuration, if required, MUST be changed to ensure security event log size does not overwhelm the system.
8.4.2.	System owners MUST identify and record the event types and attributes of their environment.

8.5. User Requirements

Reference	Security Control Requirement
8.5.1.	Access by privileged users to any system MUST be logged.
8.5.2.	Events relating to privileged user access, such as users attempting to access a resource, MUST be logged.
8.5.3.	Privileged users MUST be prohibited from accessing or modifying logs which may contain information about, or actions carried out by; those users or their accounts.
8.5.4.	System administrator and auditor privileges MUST not reside with the same individual. Administrator MUST not be able to delete, modify or disable logs.
8.5.5.	Individual responsible for reviewing log data MUST not have privileges to originate the log event.
8.5.6.	Anyone authorised to access log data MUST only be granted read-only access. In an exception case, write access should only be given to application and system needing it and MUST be notified and agreed to the appropriate team.
8.5.7.	Where log data is retained by third parties, the contracting party MUST define an appropriate access policy and document the role of each provider.

8.6. Log Management

Reference	Security Control Requirement
8.6.1.	Logs to be monitored MUST be continuously forwarded to a centralised log collection point in real-time.
8.6.2.	Any and all logs mandated by this or other standards MUST be monitored.
8.6.3.	Logs MUST be protected against deletion and tampering, both at rest and in transit.
8.6.4.	Logs MUST have the same level of protection as the system and data from which they originate.
8.6.5.	Log data MUST be reviewed routinely by analyst depending upon the event being audited.
8.6.6.	Deleting and modifying of logs of own activities MUST be detected and alerted immediately.

Reference	Security Control Requirement
8.6.7.	Performance alerts generated for things like network management MUST also be forwarded to the protective monitoring log aggregation point.

8.7. Log Retention Period

Reference	Security Control Requirement
8.7.1.	Log data MUST be retained in accordance with the department's retention policy.
8.7.2.	Log data MUST be preserved beyond the normal retention period if used for investigation purposes.

8.8. Log Archiving

Reference	Security Control Requirement
8.8.1.	Log data MUST be archived if the retention period is relatively long (e.g. over a year). Logs MUST be saved and moved to another storage space able to provide long term storage of logs.
8.8.2.	The archived logs MUST be adequately protected. For example, unauthorised access MUST be prevented; appropriate controls MUST be implemented to prevent damage to the media.
8.8.3.	The integrity of log data MUST be verified and preserved.
8.8.4.	Archived log data MUST be capable of being made available to DWP Authorised Personnel or other Government Delegated Personnel upon request.

8.9. Disposal of Logs

Reference	Security Control Requirement
8.9.1.	Log data MUST be disposed of in accordance with the department's security classification and NCSC Secure Sanitisation of Storage Media.

8.10. Log Storage

Reference	Security Control Requirement
8.10.1.	Logs MUST be stored offline in a location where access to the logs are made available in a timely manner.
8.10.2.	Stored logs MUST be protected against deletion and tampering. Changes to log data MUST be monitored.

8.11. Log Backup

Reference	Security Control Requirement
8.11.1.	Backed up log data MUST have the same level of security controls as the original data.
8.11.2.	Backup log data MUST be tested once a quarter to ensure that the data is still readable and in correct format.

8.12. Log Investigation Management

Reference	Security Control Requirement
8.12.1.	Appropriate security measures MUST be in place to protect and preserve the log data.
8.12.2.	Any log incident investigation MUST be according to the Security Incident Management Standard.

9. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 24 months of the approval of the standard.

10. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

11. Security Standards Reference List

Document Name	Location	Version
Exceptions Process	Blueprint Online / Policy & Standards Intranet page	N/A
SS-007 Security Standard - Use of Cryptography Standard	Blueprint Online / Policy & Standards Intranet Page	1.0
SS-014 Security Standard – Security Incident Management	Blueprint Online / Policy & Standards Intranet Page	1.0

12. Reference Documents

1. Security Monitoring: Business Objectives and Security Requirements, August 2016
2. GPG 13 - Protective Monitoring for HMG ICT Systems, Author: CESG, October 2012
3. NCSC Secure Sanitisation of Storage Media, September 2016

13. Definition of Terms

Term	Meaning
Monitoring	Assessing information contained in logs in real or near-real time to identify anomalies, patterns, or events of interest

14. Glossary

Acronym	Meaning
DA	Design Authority (part of Digital Group)
ICT	Information Communication Technologies

15. Controls Mapping

The requirements in this standard are derived from the high-level controls prescribed in the DWP Controls Catalogue.