Department for Work & Pensions

ThinkSecure

# DWP Protective Monitoring Security Policy

Version 1

## Contents



## 1. Overview

The high-level principles and objectives of this policy are that:

1.1. DWP information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

1.2. The DWP and all contracted third-party suppliers will record important security-related events in logs, which will be stored centrally, protected against unauthorised change, and analysed on a frequent, regular basis, by system and/or security specialists, using a combination of automated and manual methods.

1.3. The objective is to Identify, Protect, Detect, Respond and Recover (i.e. perform NIST-CSF functions) from malicious or anomalous activity or behaviour, and suspected security incidents, in a timely manner, reporting as appropriate (e.g. via the DWP Security Incident Response Team (SIRT) or to the Authority), and supporting forensic investigations where required.

1.4. The policy presents protective monitoring and log management principles from a high-level viewpoint, and it is not a step-by-step guide to implementing or using log management technologies.

1.5. The policy seeks to support DWP business in understanding the need for sound protective monitoring and security log management. It should be read in conjunction with the DWP Protective Monitoring Technical Security Standard (SS-012), which also aims to provide practical, real-world direction on developing, implementing, and maintaining effective log management practices throughout the Department.

1.6. The policy requires the DWP to establish and maintain ongoing situational awareness across the enterprise through the centralised collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the Department will have “blind spots” in it’s situational awareness that could lead to system compromise, data exfiltration, or unavailability of essential computing resources.

# 2. Definitions and Scope

## Definitions

2.1. A log is a record of the events occurring within an organization’s systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system, device, or network host.

Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software such as antivirus software; devices such as firewalls; software such as intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and software application events.

2.2. A security event is an observed occurrence in a network or information system that has a possible security relevance. e.g. minor malware infection cleaned by anti-virus tools or administrator logging in.

2.3. A security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. A security incident can result in a data breach.

2.4. A data breach is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data transmitted, store or otherwise processed.

2.5. Information Security Continuous Monitoring (ISCM) means maintaining ongoing awareness of information security vulnerabilities and threats to support organisational risk management decisions.

## Scope

2.6. The policy covers several topics, including the need to establish accountabilities and responsibilities for log management and protective monitoring, for the establishment of log management infrastructures and processes, and for the continued development and implementation of security event monitoring and management services in the DWP.

2.7. This policy does not replace any legal or regulatory requirements.

2.8. This policy applies to any and all contractual agreements for the provision of protective monitoring and log management infrastructure and processes for the Department, and these policy statements supplement all currently applicable contractual agreements to Departmental computing and networking services, including provided through managed services.

2.9. This policy applies to:

a) DWP staff, (including contractors, consultants and other workers), involved in identifying the metadata, data and information that needs to be logged or recorded; events that need to be reported; and alerts that must be generated in response to anticipated attacks to DWP ICT systems, networks and applications;

b) DWP staff, (including contractors, consultants, and other workers), involved in the determination of:

- what should be monitored,
- what should be recorded,
- how logs may be used, and
- what should be investigated in order to respond to perceived security incidents to ICT systems within the DWP estate, specifically DWP assets being monitored by the DWP Security Monitoring & Investigations Team;

c) all contracted third-party suppliers, whose systems or services may be required to provide logging, log management, log analysis, security monitoring, event management, security triage and incident response and management to ensure the appropriate levels of assurance for the confidentiality, integrity and availability of the Department's assets, including data.

## 3. Accountabilities and Responsibilities

3.1. The DWP Chief Security Officer is the accountable owner of the DWP Protective Monitoring Security Policy and is responsible for ensuring its maintenance and review, through the DWP Deputy Director for Security Policy and Data Protection.

3.2. This policy requires DWP Digital, DWP Operations Functions, and any contracted accountable parties (*see below), to clearly agree accountabilities and responsibilities for establishing data and implementing documented procedures to provide security events and log management processes in compliance with the DWP Protective Monitoring Technical Security Standard (SS-012).

*Accountable parties are people and parties that run or host systems on behalf of DWP.
For example, the system owner is accountable for ensuring relevant security events are captured in the service and the provision of log data to the agreed data store.

3.3. This policy requires the DWP Cyber Resilience Centre to be accountable and responsible for log analysis, security monitoring, and security event management.

3.4. This policy requires DWP Digital and DWP Operations Functions to be accountable and responsible for building relevant security events into their services aligned to service risk assessments.

## 4. Policy Statements

4.1. DWP Digital and DWP Operations Functions and any contracted accountable parties are required to ensure all DWP IT operating systems, devices, and appropriate software capabilities (including SaaS, PaaS, and cloud-based deployments), are configured to produce event logs to identify security-related events.

4.2. Accountable and responsible parties in DWP Digital are required to have in place processes to monitor progress on implementation of security event logging and log management processes.

4.3. Accountable and responsible parties in DWP Cyber Resilience Centre are required to have in place processes to monitor progress on implementation of protective monitoring and security event management so that they are satisfied that the requirements of this policy are being fulfilled.

4.4. DWP systems and services and those implemented on behalf of DWP must be configured to meet the requirements of the DWP Protective Monitoring Technical Security Standard (SS-012), including to:

a) enable event logging, using a standard format
b) generate appropriate event types
c) incorporate relevant event attributes in event entries
d) use a consistent, trusted date and time source to ensure event logs use accurate timestamps.

4.5. Security-related event logging must be protected from unauthorised access and accidental or deliberate modification/overwriting, in compliance with the DWP Security Standard - Privileged User Access Controls SS-001 (part 2).

4.6. Mechanisms must be established so that storage space is allocated based on expected volumes of event information.

4.7. Security-related event logs must be:

a) reviewed regularly e.g. to help identify suspicious or unauthorised activity) – see security event management below;
b) archived regularly or set to overwrite (e.g. using a rotation schedule);
c) retained according to the DWP Information Management Policy;
d) stored securely and encrypted where appropriate (e.g. to support evidence handling and possible forensic analysis at a later date).

4.8. Security-related events (stored in event logs) must be extracted to a central store (e.g. using an automated security information and event management (SIEM) tool or similar log management tool).

4.9. The logging of security-related events must be regularly reviewed to verify that the logging works as intended and has not been tampered with.

## Security Event Management

4.10. A security event management process must be established to identify, investigate, and help respond to security related events (including indicators of compromise (IOC) where appropriate), which will be provided and maintained by the DWP Cyber Resilience Centre (CRC).

4.11. The security event management process must be documented, implemented, and supported by DWP CRC and DWP Digital:

a) security practitioners who are skilled and experienced in managing security events e.g. cyber security analysts or threat analysts;
b) security event management products (e.g. network scanning software, log management tools and SIEM products).
c) IT system experts who are skilled and experienced in the application or service specific events (e.g. engineers, IT operations, architects and product owners)

4.12. The security event management process should embody a core set of capabilities, including:

a) data collection and correlation (e.g. gathering, normalising and correlating data from logs, threat intelligence and other sources whilst continually tuning tools to ensure relevance is maintained);

b) detection (e.g.defining threat scenarios to monitor, developing alerts for anomalous behaviour and establishing a mechanism for the receipt of suspicious activity reports from IT practitioners, business users or external parties);
c) monitoring (e.g. reviewing alerts, escalating where appropriate and providing feedback on false positives for refinement of correlation rules);
d) security investigation (e.g. gathering additional information to assess whether a potential or actual security incident occurred, classifying the incident according to scale, impact and severity and recommending response actions);
e) incident response (e.g. mitigate business impact of security incident through remediation, apply lessons learned to enhance future performance and report details of actions taken).

4.13. Appropriate security-related event data must be collected from numerous sources, meeting the requirements of the DWP Protective Monitoring Technical Security Standard (SS-012). This will include:

a) application logs
b) system logs
c) network equipment logs
d) threat intelligence (e.g. information about adversarial threats' past, present and predicted attacks to inform decisions or actions)
e) contextual information (e.g. vulnerability scans, penetration testing results and HR feeds)
f) third party security tooling.

4.14. All data collected (e.g. event data, contextual information and threat intelligence) must be based on threat scenarios and associated use cases, defined through the risk assessments for each service.

4.15. Specific monitoring activities must be performed to help identify anomalous behaviour.

4.16 Detection of malicious or anomalous behaviour must be supported by defining scenarios that require monitoring, based on the DWP's threat profile and risk assessments.

4.17. All alerts generated must be reviewed and actioned based on agreed playbooks in agreement with the DWP Cyber Security Monitoring & Investigations Team and aligned to the DWP Protective Monitoring Technical Security Standard (SS-012).

## 5. Policy Compliance

5.1. Where protective monitoring and security log management is not able to be carried out in compliance with the requirements of this policy, this should be presented to an assigned Authority / DWP Digital Security Risk Manager or Security Architect in the first instance, and considered for submission to the DWP Digital Design Authority (DDA) advisory or governance board where appropriate.
This presentation and possible submission must be carried out prior to deployment for new systems or services 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 policy and it’s associated standard.

Exceptions to the policy or associated standard must be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

5.2. Accountable and responsible parties must be prepared and willing to evidence compliance to this policy for audit purposes, if appropriate with security log audit records from their systems and services.