Protective Monitoring Policy	
Security Classification	**OFFICIAL**
Disclosable under Freedom of Information Act 2000	No

POLICY TITLE	**Protective Monitoring**
REFERENCE NUMBER	**WMP008h**
Version	**2.0**

POLICY OWNERSHIP	
DIRECTORATE	COMMERCIAL SERVICES
BUSINESS AREA	DIGITAL SERVICES

INITIAL IMPLEMENTATION DATE	**October 2020**
LATEST REVIEW DATE	**October 2023**
NEXT REVIEW DATE:	**October 2026**
RISK RATING	**LOW**
EQUALITY ANALYSIS	**LOW**

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail contactus@westmercia.pnn.police.uk

Handling Instructions

OFFICIAL - This document must be handled and stored according to the Government Security Classifications guidance. Neither the document nor any of its contents may be disseminated further without the permission of the Information Asset Owner.

1.0 POLICY OUTLINE

West Mercia Police (WMP) consider its information a valuable asset and consequently needs it to be suitably protected to detect and prevent unauthorised disclosure, modification, removal, or destruction. If this were to happen WMP must have the capability to identify and preserve the evidence for a formal investigation that may be required for a court or tribunal proceedings. Protective Monitoring is a key component in the management of information risk. This policy explains what Protective Monitoring is and how it can assist information risk management. Protecting information is not only an organisational responsibility; it is also a responsibility which all employees, partner agencies, delivery partners, and third-party suppliers, must take seriously.

This policy supports the overarching Information Assurance Policy and its associated procedures.

2.0 PURPOSE

Protective Monitoring facilities in compliance with legislation, regulations, policy, and standards are an essential component in the risk management approach.

Effective Protective Monitoring contributes information to mandated compliance requirements such as the HMG Security Policy Framework (SPF) reports, but also provides information on the performance of security controls to support continuous improvement. HMG Security Policy Framework audit is an important part of the mandatory requirements of the SPF, including supporting mandated compliance checking and forensic readiness, and allowing auditing of user accounts.

Protective Monitoring is also an essential requirement to police the effectiveness of technical network controls supporting incident reporting for the force and Public Services Network (PSN) and the Security Assessment for Policing (SyAP). In addition, effective Protective Monitoring should enhance situational awareness and provide an increasing understanding of threats and risks. It should also ensure accountability of the use of IT and that its use is consistent with business needs, whilst incorporating a network defence capability into Digital Services (DS).

The requirements within this policy have been set out in consideration with the Code of Ethics and our force's Vision and Values of Protecting People from Harm and taking ownership, whilst strengthening each individual policing priority by supporting the protection of the confidentiality, availability, and integrity of our information assets.

3.0 IMPLICATIONS of the POLICY

Within the scope of this policy, which comprises accounting, audit, and monitoring elements, it covers those activities associated with information provided by information security controls of nominated IT systems (e.g. inspecting firewall logs, investigating operating system security alerts, and monitoring an Intrusion Detection Service) connected to the corporate network and/or PSN.

The effective operation of this policy and associated procedures will support the delivery of effective policing services, assist in reducing costs incurred through security incidents and investigations, and protect people from harm by ensuring that information is secure, accurate and available to the right people at the right time.

WMP is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to those personnel who use deploy and maintain force systems, who may be accountable for any breaches of Information Security, for which they may be held responsible.

This policy and associated procedures support compliance with legal, national, and best practice standards including, but not limited to:

- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- Official Secrets Act 1989
- HMG Security Policy Framework
- Security Assessment for Policing
- ISO27001

There is a requirement for all personnel who deploy and maintain force systems to comply with this policy and its associated procedures, and where requested, to demonstrate such compliance. Failure to comply with the policy may be regarded as a disciplinary offence and may be dealt with subject to misconduct proceedings. In serious cases, this may be treated as gross misconduct and may result in summary dismissal.

4.0 POLICY

4.1 **Data Privacy and Usage Requirements**

4.1.1 The purpose for the collection and monitoring of Protective Monitoring data is to support the identification and response to actual or potential security incidents.

4.1.2 The data collected may also be used to create sanitized management reporting where requested.

4.1.3 Where monitoring is implemented, it must be implemented in a manner not to contravene the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations).

4.1.4 Information Asset Owners (IAO) must allow for the enrolment of information systems onto the Protective Monitoring service as required.

4.1.5 The disposal of Protective Monitoring data must be carried out in accordance with the WMP Data Sanitisation and Secure Disposal Procedure.

4.1.6 The users of any systems and applications deployed within the hosted environment must be notified that monitoring of the environment and the applications to which they have been granted access is taking place.

4.1.7 A valid Data Protection Impact Assessment must be in place to cover the use of Protective Monitoring services.

4.2 **General Requirements**

4.2.1 Protective Monitoring technologies must be implemented to detect incidents arising from the following threat groups:

- External cyber threat actors;
- Insider personnel acting maliciously; and
- Insider personnel accidentally misusing IT systems.

The term ‘insider’ is used to describe WMP staff, officers, contractors, suppliers, and other personnel with legitimate access to WMP systems.

4.2.2 Specific and enhanced monitoring for misconduct purposes may also be carried out under the Lawful Business Monitoring Policy.

4.3 **Use Cases**

4.3.1 The use cases that the Protective Monitoring solution will detect must be defined by following a risk-based approach. This means that the risks to the force, along with the wider policing community have been documented, following a risk assessment process, which is updated frequently. The threats and risks identified in this assessment must be derived from a suitably qualified, experienced, and trusted Threat Intelligence service. Because the cyber threat landscape will change, use cases must be updated and recorded within the Protective Monitoring solution.

4.3.2 Whilst the list of use cases will evolve over time, core use cases, such as the following, will be maintained:

- Maintaining visibility of communication between the force’s network(s) and other networks (i.e. the Internet or third-party suppliers).
- Capturing all authentication and access attempts to domain accounts.
- Collecting asset and configuration information to detect unauthorised personnel, connections, devices, and software.
- Monitoring personnel activities for risky behaviours that could lead to a compromise of information security.

This list is not exhaustive.

4.4 **Audit Logs**

4.4.1 To support Protective Monitoring and incident investigations, audit logs from defined systems and devices must be collected, stored securely from tampering and deletion, and retained for at least six months. This will allow for the correlation of data from multiple sources and sensors.

4.4.2 A record of monitoring/ log collection points will be maintained for audit purposes.

4.4.3 As new systems are added to the force network, a risk assessment must be performed to identify whether the existing log sources and use cases are sufficient to mitigate the risks to that specific system. Any risks that are not mitigated through existing monitoring must be subject to risk acceptance or treatment through additional monitoring controls.

4.5 **Baselining and Tuning**

4.5.1 The Protective Monitoring solution must be maintained by routinely updating monitoring and alerting baselines and tuning out events to maintain a risk averse balance between false positives and false negatives.

4.5.2 Where technically feasible, a general network baseline of activity should be maintained to aid in the detection of abnormal events, for example an increase in network traffic due to mass data exfiltration.

4.6 **Incident Analysis**

4.6.1 Incidents generated by the Protective Monitoring service must be investigated/analysed by DS Operations to understand the threat vectors, cyber kill chain stage, and potential assets that may be targeted.

4.6.2 The impact of the incident must be assessed by DS Operations and consideration must be given to invoking the Cyber Incident Response Plan, where applicable.

4.6.3 Incident playbooks must be implemented and developed to ensure that guidance is in place to allow investigating personnel to apply consistency when resolving incidents.

4.6.4 Feedback must be provided to the main Protective Monitoring service provider by DS Operations to enable the service performance to be improved over time. This will also aid in tuning the service by removing or reestablishing thresholds for alert generation.

4.6.5 Where an actual or potential breach of information has occurred, a Security Incident Report must be completed by DS Operations.

4.7 **Responsibilities**

4.8 The **Head of Digital Services** is responsible for:

- The implementation/management of a formally appointed and trusted third party who will deliver the professional Protective Monitoring capabilities necessary to meet this policy; and
- Ensuring that DS Operations have defined roles & responsibilities for receiving Protective Monitoring alerts, progressing incidents through escalation or resolution.

4.9 **Digital Services Operations Team** are responsible for:

- Ensuring that the correct configuration and management of log collection services is implemented and maintained; and
- Maintaining a local response capability using formally appointed staff or trusted suppliers to progress Protective Monitoring alerts through escalation or to a resolution.

4.10 A **formally appointed and trusted third party** is responsible for:

- Alerting DS to any errors or missing configuration that may impact on the Protective Monitoring service; and
- Providing incident alerts via formally agreed channels of communication, within Service Level Agreements.

4.11 **Testing**

4.11.1 Indirect testing and adjustment of the system must occur through routine live incident generation and as the outcome of any Penetration Testing. In addition to this, DS Operations must consider how common or high-risk threats could be safely recreated to test the performance of the Protective Monitoring system and response.

4.11.2 The DS Operations team must be notified of any Penetration Tests in order to monitor for the effective performance of systems and to ensure that alerts are generated as expected.

4.12 **Legacy Services Monitoring and Policy Exemptions**

4.12.1 Under certain controlled circumstances, it may be necessary to maintain a legacy environment which is not fully compatible with the security policies of the main IT environment. A Protective Monitoring solution must be used to conduct monitoring of any legacy environments that may still exist within controlled environments. As a minimum, all monitoring of these environments must align to *CESG Good Practice Guide No:13 Protective Monitoring for HMG ICT (see appendix A)* at the boundary of these networks to mitigate against key risks.

4.12.2 Legacy services must be recorded on the DS Risk Register for further assessment and routine management.

4.13 **References**

Organisational documents supporting the Protective Monitoring Policy:

- Force Retention Schedule
- Information Assurance Policy
- Strategic Risk Management Policy
- Information Security Incident Management Procedure
- Information Risk Appetite guidance
- Data Sanitisation and Secure Disposal Procedure

Documents can be found on the WMP Intranet or copies will be made available to authorised third parties upon request to the IT Security Officer or Information Security Officer.

5.0 DOCUMENT HISTORY

Business Lead Consulted	***Date Consulted***
Simon Bennett	07/12/2023

The following have been identified as key stakeholders who will be part of the consultation exercise.

Head of Digital Services
DS Architecture Manager
DS Operations Manager
Solution Architect
DS Security Operations Manager
Critical Friends group
UNISON

6.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	**Author / Reviewer**	**Amendment(s) & Rationale**	**Date of Approval / Adoption**
		Previously approved at JNCC meeting	JNCC 18/11/2016
16/10/2020	D Archer	Reviewed minor changes, reverted to West Mercia Policy	Oct 2020
01/12/2023	D Archer	Major changes to section 4: policy to reflect change in technology and adoption of NEP.	Dec 2023

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health and Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

Appendix A

CESG GPG13: Protective Monitoring Controls

Protective Monitoring Control		Objective
PMC1	Accurate time in logs.	To provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitating collation of events between those components.
PMC2	Recording relating to business traffic crossing a boundary.	To provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.
PMC3	Recording relating to suspicious activity at a boundary.	To provide reports, monitoring, recording and analysis of network traffic crossing a boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach an ICT system boundary or other deviation from normal business behaviour.
PMC4	Recording of workstation, server or device status.	To detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of Trojan software or so called "rootkits"). It will also record indications that are typical of the behaviour of such events (including unexpected and repeated system restarts or addition of unidentified system processes).
PMC5	Recording relating to suspicious internal network activity.	To monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated the internal network.
PMC6	Recording relating to network connections.	To monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.
PMC7	Recording of session activity by user and workstation.	To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.

PMC8	Recording of data backup status.	To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or availability is compromised.
PMC9	Alerting critical events.	To allow critical classes of events to be notified in as close to real-time as is achievable.
PMC 10	Reporting on the status of the audit system.	To support means by which the integrity status of the collected accounting data can be verified.
PMC 11	Production of sanitised and statistical management reports.	To provide management feedback on the performance of the Protective Monitoring system in regard of audit, detection and investigation of information security incidents.
PMC 12	Providing a legal framework for Protective Monitoring activities.	To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right