Protective Monitoring Policy

<table>
<tr><td>Policy summary:</td><td colspan="4">This policy states the Force strategy in carrying out protective monitoring</td></tr>
<tr><td>Policy number:</td><td colspan="4">025/2020</td></tr>
<tr><td>Version control:</td><td colspan="4"><table>
<tr><th>Version</th><th>Date</th><th>Author</th><th>Rationale</th></tr>
<tr><td>2</td><td>02.10.2020</td><td>Dean Cowe</td><td>Review before submitting for approval, minor amendments made.</td></tr>
<tr><td>1</td><td>05.08.2020</td><td>Dean Cowe</td><td>First version created due to requirement for Protective Monitoring Policy.</td></tr>
</table></td></tr>
<tr><td>Date implemented:</td><td colspan="4">November 2020</td></tr>
<tr><td>Review date:</td><td colspan="4">November 2021</td></tr>
<tr><td>Owner/contact:

(approved by –Board)</td><td colspan="4">Owner: Assistant Director ICT

Author: IT Security Officer

Approved by: DCC Claire Parmenter – Force Senior Information Risk Owner [SIRO]</td></tr>
<tr><td>Consultation and approval</td><td colspan="4">ICT Management
Information Security Officer
Information Manager</td></tr>
<tr><td>Welsh Translation</td><td>Yes</td><td>X</td><td>No</td><td></td></tr>
</table>

1. Statement of Policy

Protective Monitoring is a set of business processes, with essential support technology, that are in place in order to oversee how ICT systems are used/misused and to assure user accountability for their use of ICT facilities.
Examples of protective monitoring include the inspection of firewall logs, the investigation of security alerts, and monitoring of intrusion detection systems.

The main aims of protective monitoring are:

- To ensure the data integrity of the information held
- To enhance operational security
- To identify misuse
- To monitor exceptional usage
- To support intelligence led investigations
- To aid in the investigation of any abuse of position for personal gain / benefit of others
- To protect Force information and assets from malicious or accidental disclosure

DPP will deploy protective monitoring systems into their network. Users must accept that at some time their activities, whilst accessing or processing information, may be subject to scrutiny and monitoring.

This policy applies (but is not limited) to: All categories of Dyfed Powys Police employees, whether full-time, part-time, permanent, fixed term, temporary (including agency staff, associates and contractors) or seconded staff. Any employee accessing and using Force assets and property must have due regard to the contents of this policy.

2. Policy Scope

This policy should be adhered to at all times and should be read in conjunction with the Protective Monitoring Guide.

This policy and associated guide does not over-ride any existing procedures or policies nor negate any existing guidance regarding information security, data protection or acceptable use. It supplements such policies but with a specific focus on the protective monitoring of the DPP network, and the data held within or transported by it.

Securing data is of paramount importance within DPP – particularly in relation to the need to protect data in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of DPP. It is therefore essential for the continued operation of DPP that the confidentiality, integrity and availability of all

information recording systems are maintained at a level, which is appropriate to DPP needs.

Protective monitoring is a key requirement to ensure:

- Attacks can be detected, whether internally or externally, deliberate or accidental, and against technical infrastructure or services
- Reactionary measures can be implemented, by understanding the threat vector as per the above point
- Activity can be accounted for, to ensure attacks do not go unnoticed and that any non-compliance with legal or regulatory requirements (by users/systems/services) can be identified

Non-compliance with this policy could have a significant effect on the efficient operation of DPP as a result of potential/actual harm to Force systems, services and data, and could lead to legal action being taken against the Force.

3. Powers and Policy/Legal Requirements

This policy is fit for purpose in that it meets organisation requirements and is compliant with control measures as recommended under National Institute of Standards and Technology (NIST) guidance, specifically NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations. This policy also complies with recommendations provided by the National Cyber Security Centre (NCSC) in carrying out system monitoring within an organisation.

The Force will comply with the following legislation and all other legislation as appropriate, including, but not limited to:

- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation 2018
- Human Rights Act 1998
- Official Secrets Act 1989
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Freedom of Information Act 2000

Related policies, standards, procedures, practices, including, but not limited to:

- Dyfed Powys Police Information Security Standards and Procedures
- Dyfed Powys Cyber Security Policy
- Information Sharing Policy

- Data Protection Policy

EQUALITY IMPACT ASSESSMENT

Section 4 of the Equality Act 2010 sets out the **protected characteristics** that qualify for protection under the Act as follows: Age; Disability; Gender Reassignment; Marriage and Civil Partnership; Pregnancy and Maternity; Race; Religion or Belief; Sex; Sexual Orientation.

The **public sector equality duty** places a proactive legal requirement on public bodies to have regard, in the exercise of their functions, to the need to:

- eliminate discrimination, harassment, victimisation, and any other conduct that is unlawful under the Act;
- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
- foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

The equality duty applies to all protected characteristics with the exception of Marriage and Civil Partnership, to which only the duty to have regard to the need to eliminate discrimination applies.

Carrying out an **equality impact assessment** involves systematically assessing the likely or actual effects of policies on people in respect of all the protected characteristics set out above.

An equality impact assessment should be carried out on any policy that is **relevant** to the public sector equality duty. An equality impact assessment template is available here.

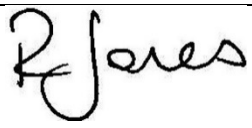
Equality Impact Assessment Completed	
Name:	Dean Cowe
Department:	Information Systems and Technology
Signed:	D. Cowe

Date:	05.08.2020

HUMAN RIGHTS ACT

CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Human Rights Act and has been reviewed on the basis of its content and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it.

Name:	R Jones
Department:	Legal Services
Signed:	
Date:	19 October 2020

4. Options and Contingencies

Policy Owner: The policy is owned by the Assistant Director ICT who will is responsible for regularly monitoring the policy for its effectiveness, challenges to the policy, any changes to NIST/NCSC guidance, and any inefficiencies in relation to the implementation of this policy.

Approval Process: Approval of decisions regarding the implementation of the policy will be made by the Information Assurance Board.

The Protective Monitoring Guide: This guide identifies the procedures and processes in relation to protective monitoring.

The procedures and processes identified within the Protective Monitoring Guide are applicable to all police officers and police staff, particularly those involved with system security and Professional Standards Department investigations. Referral to

supervisors and managers for advice and guidance will be sought where deemed appropriate.

The following Code of Ethics principles are relevant to this policy:

Accountability - We will be answerable for the decisions, actions and omissions made in relation to the application of the processes and procedures contained within the Protective Monitoring Guide.

Integrity - We will always strive to do the right thing.

Objectivity - The application of the processes and procedures contained within the Protective Monitoring Guide and the decisions made will be based upon any available evidence, recommendations and best professional judgement.

Openness - We will be open and transparent in our actions and decisions.

Selflessness - We will act selflessly and in the public interest.

CODE OF ETHICS

CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Code of Ethics and has been reviewed on the basis of its content and the supporting evidence and it is deemed compliant with that Code and the principles underpinning it.

Name:	Dean Cowe
Department:	Information Systems and Technology
Signed:	D. Cowe
Date:	05.08.2020

5. Take action and review

When carrying out protective monitoring, the ICT Department monitors the use and any abuse of Force systems and this is used to highlight any failure in the processes and procedures outlined in the Protective Monitoring Guide.
Any significant failures within the procedures contained within the Protective Monitoring Guide are referred for consideration to ICT Management.
Guidance and recommendations from relevant organisations, including NIST and NCSC will be taken into account with regards to amending/updating this policy.

This policy will be reviewed annually.

Freedom of Information Act 2000

Section 19 of the Freedom of Information Act 2000 places a requirement upon the Force to publish all policies on the Force website. Policies are why we do things and procedures are how we do them. A case-by-case review of procedures must be undertaken to protect law enforcement and health and safety considerations. Where a combined policy and procedure document is being produced the Force is legally required to publish the policy section and assess the procedure part to ensure no sensitive information is published. Generally the default position shall be that a policy and accompanying procedure document will be produced separately.

There is a requirement therefore to review this document to establish its suitability for publication. Please identify below whether the document is suitable for publication in its entirety or not. Where it is believed that disclosure will be harmful please articulate the harm that publication would cause and highlight the relevant sections within the document. Where it is perceived that there is harm in disclosure the document should be forwarded to the Disclosure Unit for review.

Suitability for publication

Suitability for publication	**Yes/No**	**Date**	**Signature**
Document is suitable for publication in its entirety	Yes	05.08.2020	D. Cowe
Document is suitable for publication in part, I have identified those sections which I believe are not suitable for disclosure and have articulated below the harm which would be caused by publication.			
Harm – in publication			

FOI review – to be completed by Disclosure Unit
(Only required if author believes there is any harm in disclosure)

Suitability for publication	**Yes/No**	**Date**	**FOI Decision Maker**
Document is suitable for publication in its entirety			
Document is suitable for disclosure in part and relevant redactions have been applied. A public facing version has been created.			
Once review has been undertaken FOI Disclosure Officer to return document to policy author and following sign–off document to be published within Force Publication Scheme. Any future changes to the document should be brought to the attention of the Disclosure Unit, as appropriate.			