Heddlu Police
DYFED-POWYS

Information Security Policy

Policy summary:	***This Policy ensures the Confidentiality, Integrity and Availability of Information received, created, and stored by Dyfed-Powys Police. This enables Dyfed-Powys Police, to share information with confidence; to have in place suitable safeguards to ensure the confidentiality, integrity and availability of Force Information Systems, whilst ensuring that all Dyfed-Powys Police's contractual, statutory and regulatory obligations for Information Security are met.***
Policy number:	***020/2020***
Version control:	***Version 1.9*** ***Date:*** *14/03/2022* ***Author:*** [redacted] ***Rationale:*** *Timely Annual Review*
Date implemented:	***14/03/2022***
Review date:	***14/03/2023***
Owner/contact:	***Information Security Officer***
Approval	***Board: Information Assurance Board*** ***Date of approval: 14/03/2022***
Final Approval	***Board: Information Assurance Board*** ***Date of approval: 14/03/2022***
Consultation and approval	***Information Management Business Area (IMBA), ICT and Legal Services***
Welsh Translation	***Yes***

Heddlu Police
DYFED-POWYS

1. Statement of Policy

The objectives of this Information Security Policy are to ensure:

- **Confidentiality** - access to data shall be confined to those with appropriate authority and protected against unauthorised access, whether deliberate or careless.
- **Integrity** - information shall be complete and accurate and protected from unauthorised modification. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - information shall be available and delivered to the right person, at the time when it is needed;
- To ensure that any use of cloud services have appropriate allocation of information security roles and responsibilities and confirmation from the cloud service provider that they can fulfil these roles and responsibilities. The force follows the guidance provided by the National Cyber Security Centre (NCSC) in relation to cloud security (see Dyfed Powys Police (DPP) Information Security Guidance);
- Secure information throughout the delivery chain;
- Ensure regulatory and legislative requirements are met;
- Ensure business continuity plans are produced, maintained and tested as far as practicable;
- Ensure information security training is available to all staff;
- Ensure all breaches of information security, actual or suspected, are reported and investigated;
- Ensure that protection is through an appropriate combination of personnel, physical, procedural and technical security controls;
- Ensure that every police activity or project considers information security as part of the overall risk management process. Any information risks must be identified and evaluated and where necessary, recorded.

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Force by:

- Identifying through appropriate risk assessment, the value of information assets, to understand their threats and vulnerabilities that may expose them to risk;

- Managing the risks to an acceptable level;
- Complying with any third party or delivery partner contract/agreement conditions relating to information security;
- Committing to achieve and maintain accreditation under the National Police Chief's Council (NPCC) Information Systems Community Security Policy and supporting Codes of Connection.
- Maintaining appropriate security standards, specifically with Her Majesty's Government (HMG) Security Policy Framework;
- Ensuring the security of protectively marked and sensitive information and information assets both belonging to Dyfed-Powys Police and entrusted to it by other organisations;
- Meeting statutory obligations e.g. UK General Data Protection Regulations (UK – GDPR) and Data Protection Act (2018);
- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies;
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities;
- Creating and maintaining within the Force, a level of awareness of the need for Information Security as an integral part of Force day to day business;
- Protecting information assets under the control of the Force.

Applicability

The policy applies (but 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. **Information Security is the responsibility of ALL employees.**

Visitors to site: Any department that has responsibility for visitors attending any Dyfed-Powys Police site must ensure that they make visitors aware of this policy and associated Standards and Procedures.

Heddlu Police
DYFED-POWYS

2. Policy Scope

Under the College of Policing Authorised Professional Practice (APP) – Information Management, the Force Information Security Officer (ISO) is responsible for the development and implementation of information security policies and procedures within the Force in accordance with:

- *The Cabinet Office Security Policy Framework*
- *Her Majesty's Government technical security standards, produced by the National Cyber Security Centre (the national technical authority for IA), and obtained via the NPIRMT.*
- *The business needs of the Force*

Compliance with this policy and associated standards, procedures and guidance, provides assurance to partner agencies, third parties and the wider community that risks to Force information are being managed to a level acceptable to the wider policing and security community.

Chief Officers, Local Policing Area Commanders, Directors and Heads of Departments are responsible for implementing the policy within their areas, and for adherence by their staff.

All employees are expected to take responsibility for the information that they create, understand its sensitivity and ensure it is handled appropriately.

3. Powers and Policy/Legal Requirements

Dyfed-Powys Police recognises that information is a primary asset of immense value to the organisation. To inspire public confidence, minimise risks to the organisation and support high quality service delivery, Dyfed-Powys Police is determined to ensure appropriate information security measures are implemented to preserve the confidentiality and integrity of all information assets.

Dyfed-Powys Police has a duty to comply with relevant legislation and regulations. All staff have an individual and collective responsibility to fully comply with the requirements of legislation pertaining to the protection of information including the security of information.

Legislation includes but is not limited to the following:

- Computer Misuse Act 1990
- Data Protection Act 2018
- UK-General Data Protection Regulation (UK-GDPR)

- Human Rights Act 1998
- Official Secrets Act 1989
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Freedom of Information Act 2000
- Crime & Disorder Act 1998
- Criminal Procedure & Investigations Act 1996

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

- Dyfed-Powys Police Information Security Standards and Procedures
- Dyfed-Powys Police Acceptable Use Policy
- Cabinet Office Security Policy Framework (May 2018)
- Dyfed-Powys Police Cyber Security Policy
- Dyfed-Powys Police Removable Media Policy
- Dyfed-Powys Police Information Sharing Policy
- Dyfed-Powys Police Data Protection Policy
- Dyfed-Powys Police Freedom of Information Policy
- Dyfed-Powys Police Records Management Policy
- Dyfed-Powys Police Data Protection Impact Assessment Policy
- Dyfed-Powys Police Retention and Destruction Schedule – Section 23 Standing Orders
- College of Policing Authorised Professional Practice (APP) – Information Management – Information Assurance

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:	[redacted] – Force Information Security & Assurance Officer
Department:	Information Management & Compliance
Signed:	[redacted]
Date:	11/02/22

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:	[redacted]
Department:	Legal Services
Signed:	[redacted]
Date:	14 February 2022

Heddlu Police
DYFED-POWYS

4. Options and Contingencies

Responsibilities for Information Security

Information Security is a responsibility shared by all members of the Force, the ultimate responsibility rests with the **Chief Constable. In their capacity as Data Controller the Chief Constable shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the UK-GDPR.**

Senior Information Risk Owner (SIRO): The **SIRO** holds the responsibility of understanding how the strategic aims of the Force, may be affected by failures in the secure use of the organisation's information systems and assets. The SIRO has ultimate responsibility for deciding the proportionality of security measures against vulnerabilities to mitigate risk.

Information Security & Assurance Officer (ISO): The **ISO** is responsible for the development and implementation of security policies, standards and procedures within the Force. The ISO is additionally responsible for co-ordinating all aspects of security, providing advice and assurance to necessitate the established information security standards necessary to safeguard Force Information Assets, as well as investigating and reporting all security incidents. The Force ISO acts as an impartial assessor of the risks that an information system may be exposed to in the course of meeting business requirements and to formally assure systems on behalf of the Force.

Senior System Owner (SSO): The Head of ICT as the **SSO**, is responsible for providing assurance to the SIRO that all Force information systems processing classified information comply with the requirements as laid down by Government, and other Regulatory bodies.

Information Asset Owner(s) (IAOs): IAOs are senior/responsible individuals within the Force who are the nominated owners of one or more identified assets, including cloud hosted solutions. They are required to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the law for public good, and provide assurance to the SIRO that the appropriate security measures are in place to protect their assets.

Data Protection Officer (DPO): The **DPO** is responsible for ensuring Force use of data is compliant with legislation, providing information and guidance on the processing of all personal data, and handling requests from data subjects in exercising their rights to access data and the rectification of any concerns. The DPO is responsible for breach notification to the Information Commissioner's Office (ICO).

Information Technology Security Officer (ITSO): The **ITSO** is responsible for protecting computers, networks, infrastructure and data from unauthorised access or damage. The ITSO provides advice on technical security architecture and posture.

Employees and Non Police Personnel: Following the provision of initial guidance and training, individual members of staff, including contracted staff and police volunteers, are required to comply with the requirements of this policy and associated working practices, including specific system Security Operating Procedures where these are in place. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard. Failure to do so may result in disciplinary action.

Line Managers/Supervisors: Shall be responsible for ensuring security processes are followed to protect the physical environment where information is processed or stored. They are also responsible for ensuring that their permanent, temporary staff, and contractors are aware of the information security policy and associated standards applicable in their work areas, their personal responsibilities for information security, and how to access advice on information security matters. It is also the line manager's responsibility to make sure all staff know how to report a security breach.

CODE OF ETHICS

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

- Accountability - You are answerable for your decisions, actions, and omissions.
- Integrity – You always do the right thing.
- Honesty – You are truthful and trustworthy.
- Openness – You are open and transparent in your actions and decisions.
- Selflessness – You act 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.

Heddlu Police
DYFED-POWYS

Name:	[redacted] – Force Information Security & Assurance Officer
Department:	Information Management & Compliance
Signed:	[redacted]
Date:	14.02.22

5. Take action and review

The **SIRO** and Information **Assurance Board** are kept informed of the information security status of the Force by means of regular reports and meetings.

This policy shall be subject to audit by the Force's internal and external auditors and be used for certification purposes for the Public Services Network and the National Police Chief's Council Community Standard Policy.

The **Force ISO** who has the responsibility for this policy, updates the policy in line with relative changes in legislation, Information Security Standards, connection requirements or other relevant standards.

Compliance with this policy is monitored via:

- Incident reporting and escalation procedures
- Internal information security audits
- Independent audits (such as the Information Commissioners Office (ICO)
- Data Protection audits

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.

Heddlu Police
DYFED-POWYS

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	14.02.22	[redacted]
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.			

Outline of any harm identified 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.

Heddlu Police
DYFED-POWYS

Full Version Control

Version	Date	Author	Rationale
1	15/10/13	[redacted]	Re-written incorporating new Force policy template.
1.2	26/03/14	[redacted]	Amendment to password management.
1.3	02/12/14	[redacted]	Amendment regarding loss of mobile devices and swipe cards.
1.4	30.12.15	[redacted]	Annual Review – including amendments
1.5	03.08.17	[redacted]	Annual Review
1.6	15.05.18		Review of Policy due to implementation of Government Security Classifications (GSC) – including amendments, incorporating new Force policy Template.
1.7	17.12.18	[redacted]	Inclusion of Information Risk Assurance Procedure with 14.3
1.8	03.10.20	[redacted]	New DPP Policy Template
1.9	14.02.22		Annual Review – Timely Review including amendments