Policy & Procedure Title:	**Information Security**
Reference No:	**133-1 a issue 6**
Workstream/Business Area:	**Assistant Chief Officer – Resources**
Policy Contact/Author:	**Assistant Chief Officer – Resources**
Service Area Approval:	**Assistant Chief Officer – Resources**
Chief Officer Approval:	**Assistant Chief Officer – Resources**
Effective (Start) Date:	**10 May 2017**
Next Review Date Due:	**May 2019**
Protective Marking	**Official**

CONTENTS

Supporting Documents:

APP Guidance:

This Policy has been checked against APP and there is none in relation to the subject matter of this Policy.

1.0	**POLICY AIMS**
1.1	**Rationale**
1.1.1	This policy sets out the approach adopted to develop, manage and improve Information Security to ensure that information assets are properly protected against loss or compromise.
1.1.2	Within the context of Information Security, 'information' includes data and any form of communication recorded or transmitted in transcript or verbally, manually or electronically. In terms of tangible assets, Information Security principles extend to paper documents, computer files, electronic records, CDs, disks, drives or any other storage or processing medium.
2.0	**PROCEDURE**
2.1	**Intention**
2.1.1	Information Security is different to 'Information Management' which embraces a much broader set of administrative procedures necessary to manage the entire life of information from origin, through processing, to disposal. However, Information Security is an integral component of Information Management and for this to be effective, a consistent, well organised and properly administered structure must be established in all working environments throughout the organisation.
2.1.2	Every aspect of business will involve Information Security considerations, therefore it remains the responsibility of all people who work for or in support of Gwent Police to safeguard organisational assets and ensure that all necessary protective measures are in place.
2.1.3	In applying this policy it is also important that the breadth of protective security principles relating to information, IT, personnel and physical security are fully integrated to create sufficient depth and resilience to complement business continuity requirements and guard against all prevailing threats.
2.1.4	Finally, Information Security must take full account of a range of legislation governing the manner in which information and data is managed and protected. A common theme is 'OFFICIAL-SENSTIVEity' and, to remain legally compliant, obligations are placed upon staff to ensure that information is protected.
2.2	**General Principles**
2.2.1	The intention is to describe Information Security requirements and demonstrate the need for activity necessary to safeguard sensitive information, counter threats and comply with legislation.
2.2.2	Central to this approach is an understanding that the organisation cannot function without information, processes and networks that combine to create a complicated infrastructure. From this it is important to identify the more sensitive intelligence, operational, financial or business assets that require specific protection and to develop measures to prevent, detect and mitigate loss or compromise.
2.2.3	To balance business needs with information security requirements a proportionate

	response is necessary and this is achieved by adopting measures that preserve: a) OFFICIAL-SENSTIVEity – ensuring that information is accessible only to those authorised to have access, and protecting assets against unauthorised disclosure b) Integrity – safeguarding the accuracy and completeness of information and processing methods, and protecting assets from unauthorised or accidental modification c) Availability – ensuring that authorised users have access to information and associated assets when required to pursue Gwent Police objectives.
2.2.4	Another significant aim is to reinforce 'OFFICIAL-SENSTIVEity' and 'need to know' principles. Information supplied in confidence, developed to produce intelligence, used to support operational initiatives or connected with other sensitive business activities, must be treated in a OFFICIAL-SENSTIVE manner and only imparted to others in the official course of duties on a strict 'need to know' basis. This requirement is supported by legislation including: a) Official Secrets Acts 1911; 1920; 1989 – require staff employed for or in support of the police service to avoid unauthorised disclosure of information b) Data Protection Act 1998 - requires personal data to be properly safeguarded and not disclosed unless properly authorised and justified c) Computer Misuse Act 1990 – renders it illegal to gain access to or use a computer without authority d) Freedom of Information Act 2000 - provides for disclosure of non-personal data, subject to exemptions including the prevention and detection of crime.
2.2.5	While the intention of this policy is to identify a range of protective security measures, considerably more detail is necessary to provide practitioners with clear procedural requirements and guidance. Such detail will be contained in a series of 'Security Policies and Procedures' that will be approved by the Force Information Assurance Board. These will be published on the intranet or otherwise circulated to those who need to know the content: a) Internet access, e-mail, social media acceptable use Policy and Procedure b) Cyber Security Incident Response Procedure c) Data Protection Policy
2.3	**Threats and Vulnerabilities**
2.3.1	In adopting relevant protective measures, the nature of threats and vulnerabilities must be considered: a) Much of the work of the police service is of interest to others and, while the organisation must operate as an open public service, it is important to protect

	sensitive assets and guard against infiltration by undesirable elements including terrorists, criminals, those who attack computers and, in some cases, the media. b) As well as external vulnerabilities, the organisation must counter unauthorised or illegal internal activity including corruption or any other deliberate or accidental act or omission which could lead to loss or compromise of information.
2.4	**Challenges & Representations**
2.4.1	Challenges and representations concerning this policy should be directed to the: Force Information Security Manager, Block A, Caerleon House, Mamhilad.
2.4.2	Information Security responsibility lies within the remit of the Assistant Chief Officer - Resources. SIRO - ACOR ¦ Information Security Service
2.5	**Guidance, Procedures & Tactics**
2.5.1	OFFICIAL-SENSTIVEity: Information available to staff and others who work in support of Gwent Police is provided for official use only. Personal use or communication to unauthorised persons is not permitted. In addition, such of the information is sensitive because of its operational, business or personal content, and this demands that strict rules of OFFICIAL-SENSTIVEity apply.
2.5.2	Need to Know: Knowledge and possession of sensitive information must be limited to those who have a genuine 'need to know' to allow them to pursue their official duties. A particular rank, grade or function does not confer any right of access to sensitive assets and the key test relates to a specific 'need to know' to allow the recipient to do their job.
2.5.3	Government Protective Marking Scheme (GPMS) a) GPMS provides a consistent standard for marking sensitive assets. The GPMS classifications commence with Official, Official-Sensitive, Secret to Top-Secret.It is the responsibility of the originator to classify the asset and control initial circulation which should be limited to those who 'need to know'. Thereafter, any processing or handling of a GPMS marked asset must follow approved procedures which include secure storage and disposal methods. b) It should be noted that most Gwent Police computer systems are secure for Official information only. In addition, internal fax or email, or external email using the PNN (Police National Network) address can also handle Official material.
2.5.4	Data Protection Particular care must be taken to protect personal data and to apply the Data Protection Act principles to ensure that collection, use, retention, disclosure and

	disposal follow legal requirements.
2.5.5	Clear Desk Practice Sensitive assets including those marked with a GPMS classification must be managed in a way that prevents unauthorised access. This includes securing assets in appropriate cabinets when not in use, particularly outside normal working hours.
2.5.6	Clear Screen Practice Password protected screen savers must be activated when the user is away from their computer terminal to prevent unauthorised access to information or systems.
2.5.7	Computer Access and Passwords Staff and others working in support of Gwent Police are only permitted access to computers and systems for which they have been specifically authorised. Access permissions include the requirement to use the personal Staff ID number as well as a unique password known only to the user. Passwords must not be divulged to others, nor written down. In addition, the password configuration should not comprise obvious names or dates that could easily be associated with the user.
2.5.8	Corporate Software No unauthorised software must be loaded onto any Gwent Police systems, whether part of the network or a stand alone facility. In addition, approved software loaded onto Gwent Police systems will not be downloaded or copied.
2.5.9	Mobile Computing Mobile computing devices such as Personal Digital Organisers (PDAs), portable memory devices, laptop computers and mobile telephones that belong to Gwent Police, or contain Gwent Police data, must be properly secured at all times. Access control (e.g. PIN) must be activated and particular care taken to safeguard equipment when travelling or in a public place. Unless equipment includes specific security measures then classification of data contained on these devices must not exceed Official.
2.5.10	Removal of Assets from Police Premises Authority is required from line managers for any asset to be removed from police premises. For assets classified OFFICIAL or higher, specific authorisation is required together with arrangements to ensure that material is properly secured and safeguarded.
2.5.11	Oversight or Eavesdropping When discussing or processing issues of a sensitive nature on police premises or in public, extra care must be taken to avoid oversight of mobile computing devices, or eavesdropping.
2.5.12	Disposal Information assets of a sensitive nature, and particularly those containing a GPMS marking, must be destroyed using approved methods. OFFICIAL and OFFICIAL-SENSTIVE material can be placed in OFFICIAL-SENSTIVE waste bins, whereas SECRET material must be shredded. Please refer to the Force Disposal Policy which can be found on the Intranet.
2.5.13	Breaches of Security Any security incident or occurrence that has the potential to compromise the organisation, staff, information or other assets, must be reported to the Force Security Manager for assessment and decision regarding further action. Reporting of incidents can be done through the Portal on the Intranet home page: http://intranet/support/is/icu//info_security/incidentreporting/index.asp

3.0	**LEGISLATIVE FRAMEWORK**
3.1	• Official Secrets Acts 1911; 1920; 1989 • Data Protection Act 1998 • Computer Misuse Act 1990 • Freedom of Information Act 2000
4.0	**HUMAN RIGHTS**
4.1	This Procedure has been checked for compliance with the Human Rights Act; with particular reference to the legal basis of its precepts, the legitimacy of its aims, the justification and proportionality of the actions intended by it, that it is the least intrusive and damaging option necessary to achieve the aims and that it defines the need to document the relevant decision making processes and outcomes of actions.
5.0	**WELSH LANGUAGE STANDARDS**
5.1	This Policy aims to comply with the Welsh Language Standards in terms of dealing with the Welsh speaking public, impact upon the public image of the organisation and the implementation of the Welsh Language Standards.
6.0	**HEALTH AND SAFETY**
6.1	The Gwent Police Service Dynamic Risk Assessment should be applied as necessary. A training package in the use of risk assessment will be provided to all police personnel if requested or required.
7.0	**REVIEW/RESPONSIBILITIES**
7.1	The policy business owner maintains outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.
7.2	The policy should be considered a ‘living document’ and subject to regular review to reflect upon any Force, Home Office, NPCC, legislative changes, good practice (learning the lessons) both locally and nationally.
8.0	**LINKS TO OTHER POLICIES/PROCEDURES/OTHER DOCUMENTS**
8.1	Internet access, e- mail, social media acceptable use Policy and Procedure; Cyber Security Incident Response Procedure; Remote Access Policy; Data Protection Policy
9.0	**APPENDICES**
9.1	None.