Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI0516
Policy Ownership	Ops Support Department
Issue Date	10/11/2016
Review Date	5 years from issue date
Governing Service Policy	Information Management
Cancellation of	SP18/2010 Information Assurance
Classification	**OFFICIAL [PUBLIC]**

SI0516

Information Security

This Service Instruction clearly defines the Information Assurance responsibilities of the Police Service of Northern Ireland and ensures the organisation meets mandatory obligations.

Keeping People Safe

Table of Contents

Table of Appendices

1. Objective

The objective of the Service Instruction is to clearly define the Information Assurance (IA) responsibilities of the Police Service of Northern Ireland (PSNI) and ensures the organisation meets mandatory IA obligations of Her Majesty's Government (HMG) and the National Police Chief's Council, Information Systems Community Security Policy

2. Definitions

'**Information Systems'** are the Information Technology (IT) and manual systems, electronic and hard copy Information Assets and the supporting business processes that facilitate the use and management of information for lawful business purposes;

'**Information Users'** are all individuals who have access to or use of PSNI Information Assets and Information Systems. Including, but not limited to, PSNI officers and police staff, temporary workers, contractors, suppliers and representatives from other organisations who process PSNI information or process information on behalf of the PSNI; and

'Information Assets' take many forms. Examples of which are in Appendix B

3. Applicability

All Information Users must ensure that all Information Assets collected and produced through PSNI business operations are processed, stored, transmitted and managed securely in accordance with HMG Information Assurance/Infosec Standards. For all PSNI Information Assets and Information Systems, the following principles must be adhered to:

- PSNI Information Assets and Information Systems must only be accessed for legitimate PSNI business purposes and only where the individual has a 'need to know';

- PSNI Information Assets and Information Systems must not be used for personal use, personal gain or illegal activities.

4. Threats

Threats to Information Assets and Information Systems emanate from many internal and external sources. These threats may manifest themselves via the unauthorised activities of personnel, the interception of communications, physical disruption and unauthorised penetration of systems both internal and external. All such breaches of security may result in the loss

of confidentiality, integrity and/or availability or the incorrect repudiation of information and information assets. If any of the threats described above occur then the consequences can manifest themselves in various ways e.g. a risk to a group or individual's safety and liberty; a disruption to emergency service activities; hinder the detection, impede the investigation or facilitate the commissioning of crime; cause convictions for criminal offences to be declared unsafe.

5. Risk Assessment Process

The Chief Constable is required to address information risk on an annual basis and must include this in the PSNI Annual Statement on Internal Control. The Assistant Chief Constable, Operational Support fulfils the role of Senior Information Risk Owner supported by the Information Security Unit assessing the information risk associated with each business process.

6. Information Security Standards

The PSNI has established this Service Instruction underpinned by a series of IS standards which provide detailed procedure on specific IS controls, countermeasures and practices which must be adhered to. This provides the assurance that Information Assets are protected and that Information Systems are operated and secured in a consistent and proportionate manner.

All PSNI Information Users must ensure that they have read and understood those standards which are relevant to their area of work and the facilities they are using.

Failure to comply with this Service Instruction or associated standards may lead to an investigation, which could result in disciplinary action and criminal or civil proceedings.

The IS standards are divided into a number of categories and are listed in Appendix A. For the avoidance of doubt, those Information Users who are part of a Specific User Group and/or have an Administrative and/or Privileged Access role on an Information System, must read and adhere to the 'All User' standards in addition the 'Specific User Group' and/or 'Technical' standards relevant to their area of work.

Appendix A Information Security Standards

Standards for All Information Users

IS STANDARD	DESCRIPTION	READERSHIP
Acceptable Use	Defines the security and use of all PSNI's information and IT equipment.	
Anti-Malware - Users	Defines users' restrictions to the introduction of software to systems and specifies procedures to be followed in respect of when and how to use anti-malware software. This area is split into two Standards; a user Standard and a technical Standard.	All Information Users
Bluetooth	Defines the acceptable usage procedure for Bluetooth.	All Information Users
Contractors and Consultants	Defines the Information Assurance procedures in respect of using contractors and consultants on PSNI's premises and projects.	All Information Users
Cryptography - Users	Defines the PSNI's approach to the use of Cryptographic material.	All Information Users
Email Usage	Defines the acceptable email usage procedure for all staff.	All Information Users
Incident Identification and Reporting	Defines the procedure for the identification and reporting of Information Security Incidents.	All Information Users
Information Security	Defines the PSNI's approach to Information Security and supplements the information presented in the IS Service Instruction.	All Information Users

Internet Usage	Defines the acceptable Internet usage procedure for all staff.	All Information Users
IT Account Management - Users	Defines process governing usernames, passwords, access to systems etc. This is split into two parts – a user and a technical guide.	All Information Users
Security Classification	Defines the PSNI's procedure in respect of applying HMG security classification to Information Assets.	All Information Users
Removable Media	Defines procedures in respect of the use of authorised removable media (e.g. CD-ROMs, USB, etc.)	All Information Users
Secure Information Asset Disposal	Defines the procedures for the secure disposal of PSNI information assets.	All Information Users
Telephony	Defines the procedures on the use of telephony systems in the PSNI.	All Information Users
WLAN, incl. WiFi	Defines the procedure on the use of WLAN and WiFi technologies in the PSNI	All Information Users

Standards for Specific Groups of Users

IS STANDARD	DESCRIPTION	READERSHIP
Forensic Readiness	Defines the PSNI's internal approach to the collection, preservation, protection and analysis of digital evidence to be effectively used in legal matters, security investigations, in disciplinary matters, in an employment tribunal or in a court of law.	Relevant only to those Information Users who have responsibility for agreeing, designing, implementing or managing Forensic Readiness arrangements
Remote Working with PSNI Information Assets	Defines Information Security Procedures for working on PSNI Information Assets outside of Police Service premises.	Those with authorisation to work with PSNI Information Assets outside of PSNI's premises
Information Incident Management	Defines the procedures for the management and onward reporting of Information Security incidents.	Incident Management Group only
Information Transfer	Defines the Information Security requirements for secure information transfer between systems or between PSNI systems and other authorised systems.	Those information users who have responsibility for approving or facilitating internal information transfer or information transfer between PSNI information systems and other authorised systems
Protective Monitoring	Defines the PSNI's internal approach to monitoring the use of Information Assets and Information Systems and to assure user accountability in their use.	Relevant only to those Information Users who have responsibility for agreeing, designing, implementing or managing Protective Monitoring arrangements

Security Clauses for Contracts	Defines the Information Security requirements to be considered and incorporated within procurement processes and contracts.	Those involved in the preparation, negotiation or reviewing of contracts relevant to Information Assets and/or Information Systems
Privacy Impact Assessment (PIA)	Provides specific procedure on the process for determining whether a PIA is required, and if required, on the creation of an appropriate PIA.	Those involved in a new initiative or process, where it is believed that there may be an impact upon the privacy of an individual or individuals

Technical Standards for System Administrators

IS STANDARD	DESCRIPTION	READERSHIP
Anti-Malware – Systems Administrators	Defines users' restrictions to the introduction of software to systems and specifies procedures to be followed in respect of when and how to use anti-malware software. This area is split into two Standards; a user Standard and a technical Standard.	All System Administrators
Application and Operating Systems (OS) Hardening	Defines how applications and operating systems should be configured to increase system security.	All System Administrators
Auditing and Accounting	Defines the requirements for the monitoring/audit of systems.	All System Administrators
Cryptography	Defines the PSNI's approach to the management and deployment of Cryptographic material.	All System Administrators
Information Systems Backup	Defines the guidelines and processes for the backup of all ICT systems.	All System Administrators

IT Account Management - System Administrators/ Service Accounts	Defines process governing usernames, passwords, access to systems etc. This is split into two parts – a user and a technical guide.	All System Administrators
Network Hardening	Defines requirements for the implementation of countermeasures in respect of the central network infrastructure.	All System Administrators
Patch Management	Defines the procedures and controls required to establish adequate patching of operating platforms and applications.	All System Administrators

Appendix B Information Assets

For the purposes of this Service Instruction, 'Information Assets' include, but are not limited to, the asset types in the following table:

Information Assets	
Assets on electronic media	Paper or electronic log files
Assets on removable media	Paper files
CCTV footage	Paper forms
Dictaphone/sound recordings	Photocopied information
Digital images	Photographic information
Electronic documents (e.g. Word and Excel)	Poster information
Electronic forms	Police Officer note/log books
Emails	Presentations
Film or video	Spoken conversations
Hard copy documents	Speeches or lectures
Hand-written notes	Transcribed notes
Internal or external PSNI web pages	Training materials