POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Information Security

Standard Operating Procedure

Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department	Information Management
Version Number	4.00 (Publication Scheme)
Date Published	28/09/2018

Compliance Record

Equality and Human Rights Impact Assessment (EqHRIA): Date Completed / Reviewed:	28/09/2018
Information Management Compliant:	Yes
Health and Safety Compliant:	Yes
Publication Scheme Compliant:	No

Version Control Table

Version	History of Amendments	Approval Date
1.00	Initial Approved Version	26/11/2013
2.00	Revised to reflect current standards	19/12/2017
3.00	Updated to reflect changes in data protection legislation	24/05/2018
4.00	Updated to reflect change from Password to Passphrase	28/09/2018

Contents

Appendices

1. Purpose

1.1 This Standard Operating Procedure (SOP) supports the Police Service of Scotland (hereinafter referred to as Police Scotland) Information Security Policy.

1.2 This SOP defines an overarching framework for the Police Scotland to protect the confidentiality, integrity and availability of Information Assets and Information Systems, whether electronic, manual, voice or data, either owned and operated, or accessed via equipment provided by Police Scotland.

1.3 This SOP is applicable to all staff, contractors and partners who have access to Police Information or premises. 'Staff' includes all Police officers, Police staff and contract / agency workers of Police Scotland.

2. Security Principles

2.1 Police Scotland is a member of the National Policing Closed User Group (CUG) and Enhanced Regime that provides information security standards that all UK police forces must meet and maintain. The National Policing Information Systems Community Security Policy commits police forces to base all local security policies on Her Majesty's Government (HMG) Security Policy Framework (SPF). Compliance is assessed by the Home Office through the application and submission of the National Policing Code of Connection and Accreditation documentation.

2.2 The SPF defines Information Security as the application of control measures to protect the **confidentiality**, **integrity** and **availability** of systems and services:

- Confidentiality – information is only accessed by those who have been authorised to do so for legitimate policing purposes.
- Integrity – accuracy and completeness of information and information processes is maintained so that it can be trusted.
- Availability – authorised users have access to information when and where it is needed.

2.3 The dissemination of sensitive information and assets should be no wider than is necessary for the efficient conduct of Police Scotland business and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. This 'need to know' principle is fundamental to the protection of sensitive assets. It applies both within Police Scotland and when dealing with individuals and partners external to the organisation.

2.4 Information subject to this SOP includes, but is not limited to:

- Electronic information stored on computers, disks, magnetic tapes (including audio or video) or any other electronic storage media;

- Information transmitted by electronic means, including incoming and outgoing emails and fax transmissions, video conferencing, radio or telephone traffic;
- Hard copy information including paper records, film, photographic images, whiteboards, briefing boards and notice boards;
- Spoken information.

2.5 An information system includes elements of the following:

- Physical environment (e.g. buildings, equipment, cables, etc.);
- Information and data;
- Software and hardware;
- Operational Service provision (what the system is there is achieve);
- Human resources (users).

3. Roles and Responsibilities

3.1 Police Scotland information is owned by the Chief Constable who is the Data Controller and the accountable officer for the organisation. The Data Controller has overall responsibility for the protection of personal and sensitive police information.

3.2 The Senior Information Risk Owner (SIRO) has delegated responsibility for the management and acceptance of information risk and for setting the risk appetite aligned to the national level.

3.3 Strategic Information Asset Owners (IAOs) are the business owners of the information within their areas of responsibility and are responsible for the effective use and protection of the information they are responsible for. Strategic IAOs can be Deputy Chief Constables, Assistant Chief Constables (ACC) or Directors and report to the SIRO.

3.4 Information Assurance provides advice and support to the IAOs and users in relation to information security. Information Assurance is also responsible for the development and implementation of information security policies, guidance, and accreditation of Information Communications Technology (ICT) systems and escalation of risk to the SIRO.

4. Staff Responsibilities

4.1 All staff are responsible for the protection of Police Scotland information; its ICT systems and other assets, and maintaining their operation, confidentiality, availability and integrity. Every member of staff has a responsibility to ensure information (in all formats) is protected from adverse impact on its integrity, availability, unauthorised disclosure, amendment or destruction.

4.2 All staff must read, understand and comply with the security requirements identified in this SOP and any supporting system-specific SOP or Data Standards, including relevant legislation, that must be followed at all times. This includes, but may not be limited to:

- The Official Secrets Acts 1989;
- Data Protection Act 2018
- The Computer Misuse Act 1990.
- The Human Rights Act 1998

4.3 Failure to do this could jeopardise the security of the systems / assets and may result in disciplinary action.

4.4 **Each time** a user logs onto a network (and for some systems) they are presented with a **User Declaration**. By clicking 'OK' a user is asserting they have read, understood and will comply with the requirements of the policies and SOPs relevant to them and the system(s) and network(s) they are authorised to access, and that they have been trained and are competent in their use.

5. System Administrator Responsibilities

5.1 System Administrators are the senior users of the system, or those who have the highest level of role based access. The Administrators have the ability to create Users and to edit or delete roles or records within the system. They are, therefore, responsible for the integrity of the information and for ensuring the correct access by users.

5.2 System administrators **must** follow any system or network specific SOPs. They **must not**, without authorisation from the ICT change management group:

- Escalate permissions or privileges;
- Bypass system security controls;
- Use an Administrator account to perform non-administrator tasks; or
- Disclose Administrator passphrases.

6. Computer User Accounts

6.1 Principles and processes for allocating, amending and removing user access rights are set out in the ICT User Access and Security SOP.

6.2 In order to log on as a network or system administrator, staff must be an authorised administrator and be in possession of system logon credentials allocated to them.

6.3 Normal users will be provided a unique logon 'User Name' and passphrase before being allowed to access information systems. Logon and passphrase details must **not** be shared with any other person to allow access to another individuals account.

6.4 Access to systems for users will be granted relevant to their post through role based access and associated system privileges.

6.5 System, network access and changes to role based access levels out with the user's normal business use must be submitted with line management approval via the IT Connect system.

7. Acceptable Use

7.1 Staff must only:

- access those systems and information to which they have been authorised;
- use the transactions for a legitimate, policing or business purpose;
- use any knowledge or intellectual rights obtained for authorised policing or business purposes.

8. Information Classification, Marking and Handling

8.1 Police Scotland processes all information in accordance with the Government Security Classification (GSC). For further information on this, please refer to the Government Security Classification (GSC) SOP.

9. Secure Destruction

9.1 Police Scotland information and asset destruction processes and methods are detailed within the Secure Disposal and Destruction of Data SOP.

10. Passphrase / Password

10.1 Access to a system is generally via a username and passphrase or password. Where possible and practical, technical controls are deployed to enforce the use of appropriate passphrases or complex passwords. Where this is not possible, users must select strong passwords to protect the system and its data. The same Passphrase or password (or the same passphrase root) must not be used for any other system or service.

10.2 When creating a passphrase users could pick something you know and can easily remember, for example: a phrase from a book you like or a place of interest. However do not use names especially you're own or anything that can identify you or your family.

10.3 Staff should use a combination of the following characteristics to create a passphrase:

- Must be a minimum of 15 characters long with no limit on length;
- Must be alphanumerical and contain both a capital letter and lower case letter. (e.g., a-z, A-Z). Good practice would suggest the use of spaces in the passphrase as a special character;
- Must not be easily guessable or contain personal information including PSI or shoulder numbers;
- Must be unique to the user;
- Must never contain the words `password', `passphrase' or `Police Scotland';
- Must never identify the individual user, department, organisation or system it will provide access to.

10.4 Complex Passwords

Systems that currently require a complex password should continue to create them to the following criteria:

- Must contain both upper and lower case characters (e.g., a-z, A-Z);
- Must be alphanumeric (contain number and letters);
- May contain symbols (For example: £ (pound sign) $ (dollar sign) € (euro sign) # (hash sign) @ (at sign) or ^ (circumflex sign);
- Must be at least nine characters long;
- Are not a word in any language, slang, dialect, jargon, etc.;
- Are not based on personal information, names of family, etc.;
- Under no circumstances must the word **Password** be used.

10.5 Once passphrases or passwords are selected they should be remembered. However, where there is a need to write them down it should be kept securely. The written passphrase or password must be protectively marked and handled at the same security level of the information held on the system and stored securely.

10.6 The majority of systems prompt staff for a password change at regular intervals. This is normally every 45 days and will not allow the previous five passwords to be used again. Passphrases will be changed annually unless there is a compromise or significant change to the policy.

10.7 Initial passphrases or passwords issued to new staff will be set to automatically force them to select a new passphrase or password when they log on to the system for the first time.

10.8 All new Police Scotland systems must be configured to adhere to the Police Scotland passphrase procedures.

10.9 Any suspected compromise of passphrases or passwords should be reported as a security incident immediately. For further information refer to the Security Incident Reporting and Management SOP.

10.10 Rules on the management of passphrases and passwords that all staff must follow are:

- Passphrases or passwords are not to be reused;
- Do not reveal a passphrase or password over the phone to **anyone;**
- Do not reveal a passphrase or password in an email message passing over the Internet;
- Do not allow anyone to watch you enter it;
- Do not reveal a passphrase or password to system / applications Managers;
- Do not talk about a passphrase in front of others;
- Do not hint at the format of a passphrase or password (e.g., "my favourite pop group and the year that they started");
- Do not reveal a passphrase or password on questionnaires or security forms;
- Do not print it out;
- Do not share passphrases or passwords;
- Do not allow anyone else to use your passphrase or password to access a system or network;
- Do not use the same passphrase, nor a common passphrase root/string on any other system or service.
- Administrators must not use their admin passphrase for use with their normal account.
- Users must lock their terminals when out of the office or away from their desk.

10.11 If you need further information or guidance please contact the **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35 Law Enforcement** and a member of the Information Assurance team will respond to you directly.

11. Copy and Paste

11.1 Staff must **not** copy and paste protectively marked data from a system to another one of a **lower** protective marking, including the Internet and email systems.

11.2 To avoid the risk of a security incident, when 'Copying and Pasting' **confidential** data into a system or application having a lower security classification than the original, the data **must** be sanitised on the higher level system, **before** being copied.

11.3 Where the copy and paste functionality is disabled, users must **not** circumvent the controls without authorisation or it being detailed in a system specific SOP. This is particularly important when copy and pasting data that includes personal (nominal) data.

12. Printing

12.1 Staff must ensure that they are aware of the potential for accidental disclosure through the careless use of protectively marked print outs.

12.2 Staff must **not** leave protectively marked printing on or near a printer. It must be picked up straight away after printing.

12.3 Multi Functional Device printers (MFD) must have pin code functionality enabled to restrict the release of prints to the authorised user when they are present at the device. Use of this method for printing is to prevent information being left sitting on printers in areas where the MFD is in a shared location and users located in the office do not have a 'need-to-know' about the material.

13. Clear Desk Policy and Overlooking

13.1 Police Scotland operates a 'clear desk' policy.

13.2 Information left on desks is open to casual reading by others working in the vicinity or by third parties visiting the premises. All 'Protectively Marked' or sensitive information must be locked away when the desk is unoccupied or at the end of the day and prevent overlooking.

13.3 Paper and computer media must be stored in suitable locked cabinets when not in use, particularly outside working hours.

13.4 'Protectively Marked' or sensitive information held on white boards and notice boards must be covered when not in use to prevent unauthorised access by those who do not have a need to know.

13.5 Staff must ensure that when working on an ICT system:

- The keyboard, computer screen or device (i.e. Blackberry) they are working on cannot be overlooked by unauthorised individuals who do not have a need to know;
- They do not leave a device or computer terminal unlocked when unattended;
- Log out of a system or application when finished.

14. Encrypted Mobile Devices

14.1 All removable media devices must be encrypted to the correct standard appropriate to the classification of the information held on it. For further advice on encryption products contact the Information Security Manager **Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 35 Law Enforcement.**

14.2 For handling instructions for specific encrypted solutions, i.e. encrypted laptops, refer to the Mobile Data and Remote Working SOP.

15. Desktop and Laptop Shutdown Procedures

15.1 Unless stated otherwise, all desktop PCs should be powered down at the end of the working day.

15.2 All computers must be 'locked' when not attended by using the 'Control-Alt-Delete' function ('Ctrl' + 'Alt' + 'Del' keys, pressed simultaneously).

15.3 Staff using a laptop within the Police Scotland estate **must** power down the laptop at the end of the working day.

15.4 Staff using a laptop **outwith** the Police Scotland estate **must** not leave the laptop unattended. Power down the laptop and ensure it and any Remote Access Service (RAS) equipment is stored as per the Mobile Data and Remote Working SOP.

16. Removal of Information Assets from Police Scotland Premises

16.1 Staff are **not** permitted to remove police information or other assets from the Police Scotland premises unless:

- The information, equipment or other asset is part of an approved remote working arrangement.
- The member of staff is allocated a mobile device, for example: Blackberries, mobile phones, Personal Digital Assistants (PDAs), CD /

DVD Writable / Re-Writable Devices, digital cameras and their memory cards, Universal Serial Buses (USBs) as part of their job role.

- The member of staff is authorised to do so as part of working arrangements for their job role.

16.2 For specific handling instructions on authorised ICT devices, i.e. Blackberries, USB pens etc. refer to the Mobile Data and Remote Working SOP.

17. Personal or Unauthorised Equipment

17.1 Under **no** circumstances must any personal or other unauthorised third party ICT system or device, for example: USB pens / memory sticks, mobile phones, iPods, Blackberry, cameras, external memory drives, be connected to Police Scotland computer systems or networks. This poses a significant security risk as a malware (computer viruses etc.) ingress point and the potential for subsequent, unauthorised disclosure of information.

17.2 Police Scotland information **must not** be transferred or redirected to any personal or other unauthorised third party systems or device.

18. Loading Software

18.1 Software must **only** be loaded onto a system or device by an authorised member of ICT staff.

18.2 Anti-virus software is applied to Police Scotland computer equipment by ICT staff and updated on a regular basis. All staff are responsible for reporting any virus alert or suspected virus infection to the National ICT Service Desk immediately.

19. Wireless Equipment and Bluetooth

19.1 Wireless equipment (i.e. routers, PCs / laptops and keyboards) must **not** be connected to the Police Scotland networks / systems, unless authorised by Information Assurance who can be contacted at iso@scotland.pnn.police.uk.

19.2 Bluetooth must **never** be used with a computer terminal, laptop or any other mobile device that contains protectively marked data or when connected to a Police Scotland system.

19.3 Bluetooth use is only permitted for hands free telephony on Police Scotland Blackberry devices after approval from Information Assurance.

20. Monitoring and Audit

20.1 As per The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 all staff should be aware that their individual activities on systems and applications are auditable. This is supplemented by Closed Circuit Television (CCTV) and access control information. Any unauthorised activities could result in disciplinary action or criminal proceedings.

20.2 In particular, any action which may cause a breach of The Official Secrets Act 1911 to 1989, Computer Misuse Act 1990 or Data Protection Act 2018 may be considered as gross misconduct

20.3 Police Scotland recognises that electronic communications in its various forms is a rapidly changing area, offering opportunities that can provide business benefits which must be used according to the acceptable use of the system. However; all Police Scotland Staff must be aware that such systems, which are classed as electronic communications in the wider sense, whether they be owned, leased or sponsored, may be the subject of monitoring by authorised representatives of Police Scotland and there should be no expectation of privacy on the part of Staff when using them.

20.4 Authorised Staff within Information Assurance and the Anti-Corruption Unit are permitted to perform an audit of a system, its management, its system administrator personnel or its users in their adherence to this SOP or any supporting system-specific SOP.

Appendix ‘A’

List of Associated Legislation

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998
- Data Protection Act 2018
- Health and Safety at Work Act 1974
- Official Secrets Acts 1911 to 1989
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Police Service of Scotland (Conduct) Regulations 2013
- Public Records (Scotland) Act 2011
- Human Rights Act 1998

Appendix ‘B’

List of Associated Reference Documents

Policy

- Information Security Policy

Standard Operating Procedures

- Secure Disposal and Destruction of Data SOP
- Email and Internet Security SOP
- Government Protective Marking Scheme (GPMS) SOP
- ICT User Access Security SOP
- Security Incident Reporting and Management SOP
- Mobile Data and Remote Working SOP

Guidance

- HMG Security Policy Framework (SPF)

Appendix 'C'

Glossary of Terms

- CUG Closed User Group
- GPMS Government Protective Marking Scheme
- GSC Government Security Classification Scheme
- HMG Her Majesty's Government
- IAO Information Asset Owners
- ICT Information Communications Technology
- PDA Personal Digital Assistant
- RAS Remote Access Service
- SIRO Senior Information Risk Owner
- SOP Standard Operating Procedure
- SPF Security Policy Framework
- USB Universal Serial Bus