SCOTTISH POLICE AUTHORITY

Information Security Standard Operating Procedure

Version	**4.0**
Owner	**Head of Information Management**
Review Date	**May 2018**

Version Control

Version	Date	Author	Description/Amendment
V1.0	May 2013	L Davie	Final Version
V1.1	November 2015	L Davie	Review & Update
V2.0	November 2016	L Davie	Review and Update Function Titles
V3.0	November 2017	L Davie	Update roles as per ICO audit
V3.1	April 2017	F Blair	GDPR Updates
V4.0	May 2018	L Davie	Review changes

Document Review

Role Title	Draft Review (Y/N)	Review (Y/N)	Sign Off Required (Y/N)	Date
Director of Governance & Assurance	Y	Y	Y	June 2018
SMT		Y	Y	June 2018
Staff Association		Y		June 2018
Board		Y		June 2018

Distribution

Version	Date	Name(s)
V1.0	May 2013	Staff
V1.1	December 2015	Audit and Risk Committee for Approval
V2.0	November 2016	Head of Governance & Assurance
V3.0	November 2017	Intranet
V3.1	May 2018	SPA IM staff
V4.0	June/July 2018	SPA SMT,Staff Associations,
	Aug 2018	Staff

Statement

The Scottish Police Authority (SPA) is committed to ensuring the protection of information assets and as part of this aim complies with the ACPO Community Security Policy (CSP) that details the strategy for the security of information processes throughout the police community and forms a framework for other subordinate policies.

The purpose of Information Security is to ensure that the business of SPA continues uninterrupted by preventing and minimising the impact of security incidents in relation to any information held.

Information Security can be broadly defined under the following three headings:

- **CONFIDENTIALITY**
  Protecting sensitive information from unauthorised disclosure or intelligible interception

- **INTEGRITY**
  Safeguarding the accuracy and completeness of all information held

- **AVAILABILITY**
  Ensuring that information and vital services are available to authorised staff when required

Sharing personal data is an increasing business activity for SPA. Assuring the confidentiality, integrity and availability of that personal data is critical for operation of SPA functions.

Table of Contents

1 Introduction

Information is a key asset to the Scottish Police Authority (SPA) and the correct handling of information, including personal data, is vital to the delivery of support services to the Police Service of Scotland (PSoS) and other Criminal Justice partners. In striking the right balance between sharing and protecting data, SPA must manage business impacts and risks associated with confidentiality, integrity and availability of all information.

Information Assurance (IA) is the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. The IA functions that support the protection of SPA Information and Information Communications Technology (ICT) Systems are risk management, accreditation, standards and compliance. The importance of IA to public service delivery has been demonstrated by the publication of a National IA Strategy and this policy supports that strategy. The International Standard for Information Security Management Systems ISO/IEC 27001 is acknowledged as good practice and this Standard Operating Procedure (SOP) is aligned to that standard.

2 Intention

This Information Security SOP is produced to ensure the SPA can meet the requirements set by HM Government and our stakeholders to process information across our networks and link to the Public Services Network (PSN) and other Criminal Justice Agencies and delivery partners.

Supporting SOPs are documented separately and must be implemented to minimise the risks to Confidentiality, Integrity and Availability as well as ensuring the necessary controls for Audit and Accountability of network and systems use.

All users of SPA networks and information systems must comply with this SOP.

Failure to comply may result in disciplinary/misconduct proceedings.

3 Method

This Information Security SOP has been produced to formalise management direction and support for the security of the SPA communications networks, connected systems and physical records. The SOP will be reviewed periodically as part of the programme of work for information security. All users must comply with this SOP and supporting system operating procedures. Users include other criminal justice agencies working in partnership with the police.

The SOP details the requirements necessary to comply with the overarching Information Management Policy (IMP), which in turn set out requirements for compliance with:

- ACPO Community Security Policy (CSP)
- Cabinet Office Security Policy Framework (SPF)
- International Standards Organisation (ISO) 27001:Code of Practice for Information Security
- Governing legislation (Data Protection Law (as defined in the Data Protection Policy)), Computer Misuse Act 1990, etc)

The SOP is effective throughout the life of our networks and systems and should be read in conjunction with:

- Network and System Risk assessment and Audit Reports as and when produced
- Network, system user and training guides as and when produced
- SPA Information Sharing Protocols as developed
- Specific Internet and Email requirements
- Security Policy Framework (provides the Government guidance for the implementation of ISO 17799/27002 controls)

- Security standards and other (HMG) IA Standards, Good Practice and Memoranda produced by the Communications Electronics Security Group (CESG) and CPNI (Centre for the Protection of the National Infrastructure).

4 Security Organisation

SPA has a Data Protection Officer supported by an Information Management team to advise on and oversee the monitoring of the information security framework, policy and supporting practices that initiate and control the implementation of security for all communications networks, systems and processes.

Access requests for information from SPA networks and systems from third parties must be risk assessed and formally endorsed by other joint data controllers where necessary.

Connection to SPA networks by 3rd parties must be authorised in writing by SPA's Data Protection Officer.

5 Information Classification & Control

The CSP and SPF require police information to be appropriately protectively marked in terms of the Government Secure Classification Scheme (GSC) or any successor to this scheme. These controls will cover sites, buildings, rooms, equipment, people and procedural security.

SPA only has the electronic facilities to process information up to and including OFFICIAL (SENSITIVE).

6 Personal Data

SPA is required to handle, protect and share large amounts of personal data. Personal data is information, which relates to a living individual who can be identified from that data (or can be identified from that data in combination with other information that is available to SPA). This mirrors the definition set out in Data Protection Law (as defined in SPA's Data Protection Policy) and includes any expression of opinion about an individual, or of intentions towards him/her.

Business areas must comply with the data protection principles set out in Data Protection Law, to ensure a high level of confidence that personal data is handled correctly. There are specific requirements relating to handling personal data as defined in HMG IA Standard No.6 – Protecting Personal Data and Managing Information Risk.

Where there is a requirement for personal data or sensitive business information to be moved out-with a secure network, encrypted SPA supplied devices must be used.

7 Roles and Responsibilities

The Chief Executive Officer of SPA has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This responsibility is supported by a Senior Information Risk Owner (SIRO) and SPA's Data Protection Officer. Day-to-day duties will be delegated to SPA Information Management (IM) Team. Technical assurance is provided as a service to SPA by PSoS.

SPA's Data Protection Officer is responsible for ensuring that SPA complies with all relevant Information Assurance legislation and sector standards by developing, maintaining and auditing SPA's information assurance activities. The DPO shall ensure that the SIRO is appropriately advised in respect of relevant risks and mitigation. Where systems are delivered by PSoS, the DPO will act as the Accreditor.

The IM Team is responsible for assisting the DPO with the co-ordination of compliance activity that supports the SPA Information Assurance Framework and providing specialist advice in respect of records management.

The Senior Information Risk Owner is responsible for assessing accreditation documents prepared by SPA/PSoS IM staff to ensure relevant risks have been captured and mitigated appropriately thus reducing the risk to SPA operations. The SIRO will co-ordinate the investigation of security incidents and ensure the appropriate recording and reporting or security incidents at local and national level. Where systems are delivered internally and assured by the DPO, the SIRO will act as Accreditor.

8 Physical security

8.1 General

SPA offices are subject to access controls to prevent unauthorised access and keep the information that we hold safe and secure. Personnel processing personal data for or on behalf of SPA should remain mindful of why these controls are in place and ensure that they are maintained at all times (e.g. the doors should not be propped or wedged open). Access controls are set out in further detail in our Access Control Policy.

Procedures are in place to help SPA personnel easily distinguish between employees and visitors. All visitors must be issued with a visitor badge that must be worn at all times when moving around the building and are subject to strict sign-in and sign-out procedures. Where it is necessary for a visitor to move through any office, he/she must be escorted at all times by an employee, because personal data and controlled information is held in these areas and it is important that this is not accessed in any way.

Where personal or controlled information is held in a physical format, it is important that this is retained in our secure cabinets or our safe. The keys for cabinets must be kept secure in a key safe (to which other staff can access). Physical format information is a high security risk. Personal and controlled information should therefore not generally be taken out of the office in a physical format except where approval has been obtained to do so (at senior management level or above) and it is kept secure at all times. To ensure an appropriate audit trail, the physical record sign-out spreadsheet should also be completed where personal data or confidential information is being taken out of the office in a physical format.

Where there is a requirement to transfer or transmit personal or controlled information in a physical form, this must be done in a secure way. Where postal or courier services are used, the information should be packaged up in an appropriately strong and durable envelope (or equivalent) to mitigate damage in transit. If packages contains special category personal data, secure courier or recorded delivery methods of postage should be employed.

Details of procedures in handling of information assets in line with the Government Secure Classification Scheme can be found in the SPA/PSoS GSC SOP.

8.2 Clear Desk Policy

A clear desk policy for papers and removable storage media has been adopted. For SPA, the term "clear desk" means that personal data and confidential information must not be left in a non-secure environment, such as on a person’s desk.

In order to protect information assets from theft or damage (e.g. flood or fire), the following controls are in place:

- Fax machines and printers that are likely to receive personal data and confidential information are to be adequately protected and located within office environments.

- All faxes and printouts are to be collected as soon as possible.

- At the end of each working day, desks are to be cleared of documents and papers containing personal data and confidential information. These documents and papers are to be stored as appropriate in an individual's desk or in filing cabinets.

- All personal data and confidential information which is to be shredded should be placed in the confidential bins when no longer required. This includes any financial data.

- Files and other storage media are to be treated in the same way.

- All employees are accountable to the DPO as per our Data Protection Policy.

8.3 Network Security

Access to SPA's network (and all of our electronically held records and information) is controlled by a user authorisation procedure. The level of access that is provided (ultimately by our IT Support provider – PSoS) is controlled through this authorisation procedure which is subject to an HR process and approval at senior manager level or above. Access rights are administered by the PSoS Technical Support Team.

Users are provided access only to the information or systems that are required to fulfil the role. When a user leaves SPA employment, all of their system log-ons must be immediately revoked and any other access to information via PED's way must be immediately removed. Senior managers (and above) are responsible for ensuring that such events are communicated to the IM Team and IT Support Provider so that these steps are then taken. If, due to an unexpected absence, access to a member of staff's user logon (or similar) is deemed appropriate, then this must be authorised by a member of the IM Team.

All users are required to agree to SPA's Acceptable Use Policy as part of the network logon process.

Access to systems is generally via a username and password. Where possible, practical and technical controls are deployed to enforce the use of complex passwords. Where this is not possible, users must select complex passwords to protect the networks and its data. Users should use the following rules to create sufficiently strong passwords:

- must contain upper and lower case characters
- must be alphanumeric (both numbers and letters)
- may contain symbols
- at least nine characters long
- not based on personal information

Once passwords have been set, the following guidelines must be adhered to:

- Passwords should be treated as confidential information. Do not provide or hint at your password to another person (including administrators, superiors, other co-workers, friends, and family members) under any circumstances.
- Don't let anyone see what you are entering as your password.
- If someone demands your password, refer them to this policy or have them contact the IM Team.
- Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to SPA's network or a protected Web site.
- Do not write down passwords.
- Do not use the "Remember Password" feature of applications.
- Passwords used to gain access to SPA systems should not be used as passwords to access non-SPA accounts or information.
- If possible, don't use the same password to access multiple SPA systems.
- If you know or suspect that your password has been compromised, it must be reported to the IM team and the password changed immediately.
- The IM Team may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

8.4 Hardware use

SPA equipment must be kept secure at all times and should only be accessible to other SPA users. Our hardware must not be used by, given or loaned to anyone who does not work for SPA.

Users must use a password-locked screen or log-off their laptops and other devices to prevent others from viewing information when away from their desk.

Users should not save personal or controlled information to another media source other than a business approved memory stick.

Users must take reasonable care of SPA hardware and protect it from physical damage wherever possible:

- Take reasonable and common sense precautions to avoid drinks or liquids being spilled on hardware.
- Always carry hardware in any protective bags or boxes provided.
- Do not place hardware on furniture that is not designed to support it.

Users must not use their own devices to access SPA's network.

SPA is responsible for all information stored on our hardware. No personal (non-work related) files should be saved to SPA equipment. Under no circumstances should files be stored that are covered by copyright (or other intellectual property rights) and we do not have the proper permission to use them.

Employees must ensure they return all hardware to their line manager before leaving the organisation. In other circumstances, if the requirement for equipment changes, surplus equipment should be returned to the IM Team to return to the IT Supplier.

Procedures in relation to remote working, and remote working hardware, are set out in SPA's Remote Working SOP.

9 System Security

9.1 Accreditation and Audit

Accreditation provides a risk owner with the basis to make an informed decision on whether they should accept the risks associated with a given capability, balanced against the opportunities it presents.

The role of the Accreditor is to:

- Act as an impartial and independent assessor that the risks associated with the adoption of an information system, service or business process are acceptable to the organisation, and to accredit that system on behalf of SPA.
- Ensure that the risk management process follows HMG Security Policy Framework (SPF) outcomes (reference [e]), compliance or Codes of Connection, or any other sector specific standards but ensures that the depth and rigour required is proportionate and matches the SPA's situation

ICT systems that process protectively marked data must be accredited using recognised methodology and the accreditation status must be reviewed at least annually to judge whether material changes have occurred which could alter the original accreditation decision. Further information on accreditation can be found in SPA's Information Management Strategy.

SPA must have the ability to regularly audit information assets and ICT systems. This must include regular compliance checks carried out by the Accreditor, Information Assurance experts etc. and a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system, that may be required for legal and management purposes.

All ICT systems must have suitable identification and authentication controls to manage the risk of unauthorised access, enable auditing and the correct management of user accounts.

9.2 Codes of Connection and Technical Control

SPA must comply with the requirements of any Codes of Connection, multilateral or bilateral international agreements and community or shared services security policies to which we are signatories (for example PSN Code of Connection).

Codes of Connection should cover the following technical policies:

- Patching policy, covering all ICT systems including Operating System and applications, to reduce the risk from known vulnerabilities.
- Policy to manage risks posed by all forms of malicious software ('malware'), including viruses, spyware and phishing etc.

  Boundary security devices - (e.g. firewalls) must be installed on all systems with a connection to untrusted networks, such as the Internet.
- Content checking/blocking policy.
- Lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access and functionality) than required.

Where these are not covered by Codes of Connection, or SPA are not signatories, separate policies covering these areas must be established.

9.3 Cryptography

When encryption is required, the DPO or the IM Team should be contacted for advice. Where there is an intention to take encrypted devices overseas, the 'Use of PEDS Overseas' SOP must be consulted.

All CDs/DVDs containing personal data must be encrypted in transit. Only SPA or PSoS issued encrypted memory sticks/devices are to be used for SPA business.

9.4 Procurement

Security requirements are to be specified in all contracts between SPA and other parties; and all new ICT contracts handling personal data must adhere to the relevant Government Commerce ICT model terms and conditions.

9.5 Secure Disposal

All media used for storing or processing protectively marked or otherwise sensitive information must be disposed of or sanitised securely in accordance with HMG IA Standard No.5 (or any successor to this standard) – Secure Sanitisation of Protectively Marked or Sensitive Information. Further advice on secure disposal arrangements can be obtained from SPA's IM Team

IT kit must be disposed of by ICT in accordance with the PSoS Secure Disposal SOP.

9.6 Personnel Security

Security responsibilities for the design, implementation, operation and use of SPA communications networks and systems must be included as part of job descriptions and post holder duties.

Users shall be assessed and vetted, in line with SPA/PSoS Vetting SOP, Retiral and Discharge/Dismissal SOPs.

All users shall be trained and made aware of their duties regarding network and system use in relevant areas of information confidentiality, integrity, availability, audit and accountability. Line managers are responsible for ensuring staff have undertaken appropriate training prior to accessing information assets.

A formal record or acknowledgement shall be obtained from users to confirm they are aware of and understand their personal responsibility to comply with the security policy, legislative requirements and operating procedures

9.7 Physical & Environmental

All communications and information systems equipment and files should be housed in secure areas. All SPA premises have been provided with one or more physical security barriers, reception control, door controls, CCTV monitors and intruder alarms deemed appropriate to combat the perceived physical and environmental threats

Physical security controls of sites, buildings and rooms must be maintained and kept under review to ensure they are effective. All personnel must observe and comply with entry and visitor controls.

Rooms used for encryption coding must be lockable and windows must be capable of being covered.

Further information can be obtained in the SPA Physical and Environmental Security Policy.

9.8 Communications & Operations Management

Responsibilities and procedures for the management and operation of SPA communications networks and systems must be agreed and communicated with PSoS as the service provider.

Network and system servers (and other relevant equipment) will primarily be managed centrally by the relevant PSoS IT Manager and future capacity assessed in conjunction with System Owners to ensure technical system resources are available to meet workload and processing timescales

Networks and systems will be protected from malicious software (including viruses, worms, and Trojan horses). Only authorised PSoS and SPA IT staff and contracted suppliers will maintain network and other operating system software.

The relevant PSoS IT Manager will implement routine housekeeping procedures for all centrally managed data and software. Backup copies of data and software (for all networks and systems) will be secured to a timetable agreed with the Heads of Business Area and System Owners and stored securely in secure data safes on or off-site. Housekeeping will also include recovery testing, logging and responding to faults as well as security policy compliance monitoring.

Network security facilities will be provided by the relevant PSoS IT Manager. This will include use of network management tools and where appropriate firewalls and other communications network defences (e.g. intrusion detection system) certified to standards approved by industry and government as necessary.

All employees must ensure that all paper files associated with SPA communications networks and systems are protected from unauthorised access, loss and destruction. Protective measures must also apply to audio recordings and CCTV/Video footage and photographic images.

Any exchange of information (or software) between SPA and other organisations, must be controlled and be compliant with legislation. The relevant PSoS IT Manager should control any software exchange. System Owners should generally control data and information exchanges.

9.9 System Development & Maintenance

The design, development, testing and implementation of communications networks and information systems (e.g. new devices, menus, screens and facilities) must include a separation of duty between user, developer, tester and implementer.

Security requirements to enforce this policy must be incorporated wherever possible into network and system devices and software. Security measures will need to balance cost and effectiveness and may include technical or non-technical measures that are practical and workable in the context to defend against the threats and risk assessed

Testing and implementation of equipment and software changes must be documented, assessed and authorised by the relevant PSoS IT Manager. Audit trails should be kept for critical changes to devices such as firewalls and access routers (e.g. for the PSN) and initiated as a result of approved change control procedures.

PSoS ICT staff will provide first line support for network/system problems and will invoke the appropriate second line support from contracted suppliers in accordance with the terms of maintenance agreements.

9.10 Business Continuity and Disaster Recovery Management

A Business Continuity Plan (BCP), including Disaster Recovery (DR) arrangements for key communications networks and corporate system facilities (including cryptography) must be documented in conjunction with Health and Safety and Resilience Managers and System Owners.

The plans must include early assigned roles and responsibilities for invoking and executing the plan. Essential contact details (both within and outside SPA) should be included.

Individual plans will exist for discrete areas of operation (e.g. computer/server rooms, network/PABX equipment room/s). Collectively they will guide the recovery actions needed to reconstitute network and system support services back to normal operation.

Individual System Owners must ensure that manual processes are aligned with automated processes so that in the event of network/system destruction or data loss a recovery of the most recent changes can be facilitated from source documents or communication actions.

The BCP and supporting DR plans should be tested periodically (in part or in whole) to maintain their relevance, provide confidence and ensure those responsible for implementing them are trained.

10 Compliance

Diversity

There is no adverse impact on any group in terms of race, religion, gender, sexuality, disability, or age in relation to this procedure.

Health & Safety

There are no specific additional issues in relation to health & safety relating to this procedure.

Administration

Head of Business Areas are responsible for ensuring compliance with information security requirements.

The Head of Information Management is responsible for ensuring that all relevant procedures prepared by SPA personnel are in accordance with this procedure.

The Head of Information Management is responsible for ensuring that regular audits are undertaken to ensure compliance with this policy and relevant legislative requirements.

All staff will receive appropriate training / briefings in accordance with the information handled within their job role.

Communication

These arrangements will be communicated to staff via Heads of Business Areas and will be accessible via the Intranet.

Relevant sections of the procedure will form part of SPA's Induction Pack. Where relevant and in response to any changes, additional training/guidance will be provided to all employees.

Monitoring and Review

SPA's Information Security policy and procedures will be reviewed annually by the Head of Information Management.