SCOTTISH POLICE SERVICES AUTHORITY

Information Management Strategy
SPSA 0062

Version	**V3 23rd June 2011**
Review Date	**June 2012**
Owner	**Senior Information Risk Owner**

Version Control

Version	Date	Author	Description
V1	06/03/2009	Records Manager & IAO, SCDEA	First Publication
V2	02/06/2009	Records Manager & IAO, SCDEA	Second Publication
V2.1	16/12/2010	Records Manager & IAO, SCDEA	General review throughout. Addition of other IRM roles and Appendix A.
V2.2	01/02/2010	Records Manager & IAO, SCDEA	Addition to policy number and 12.13. Change of template
V2.3	09/05/2011	Records Manager & IAO, SCDEA	Change of template
V3	23/06/2011	Records Manager & IAO, SCDEA	Third Publication

Document Review

Name	Role	Draft Review (Y/N)	Review (YN)	Sign Off Required (Y/N)
DSU Ian Thomas	DSU Intelligence	Y	Y	N

Distribution

Version	Date	Name(s)
V1	06/03/2009	SPSA
V2	02/06/2009	SPSA
V2.1	16/12/2011	SPSA MoPI Working Group
V2.2	01/02/2011	SPSA MoPI Working Group
V2.3	09/05/2011	DSU Intelligence
V3	23/06/2011	SCDEA & SPSA

SCOTTISH POLICE SERVICES AUTHORITY

INFORMATION MANAGEMENT STRATEGY,

STANDARDS AND WORKING PRACTICES

STRATEGY STATEMENT

This document underpins all the Scottish Police Service Authority (SPSA) strategies and policies inherent in managing information and provides the over-arching framework within which to implement those policies and protocols.

Implicit is the understanding that policies, procedures and processes for all key elements of information management exist including vetting, information security, systems security, risk management, records management, review, retention and disposal, disclosure, dissemination and sharing, and audit and quality assurance; and each has a policy owner and number, together with a review schedule.

Embedded is the acknowledgement of the existing legal framework for the management of information in legislation relating to Data Protection, Human Rights and Freedom of Information.

References to the management of police information include the processes of obtaining, classifying, recording, storing, reviewing, retaining, deleting and sharing information, including personal information, for police purposes in accordance with principles governing those processes.

Table of Contents

1 Introduction

Under the Management of Police Information (MoPI) Code of Practice (CoP) the Chief Executive will establish and maintain for the Scottish Police Services Authority, (SPSA), an Information Management Strategy (IMS), complying with guidance and standards to be issued under the MoPI CoP.

This IMS also applies to the Scottish Crime and Drugs Enforcement Agency (SCDEA). The Director General of the SCDEA, will establish and maintain guidance and standards issued under the MoPI CoP for the SCDEA.

The SPSA has a duty to obtain and use a wide variety of information (including personal information), in order to discharge its responsibilities effectively. This IMS and accompanying standards, in conjunction with all other information management related policies, procedures and processes, provides a mandate for the performance of all information management functions to ensure all staff, including agencies, contractors and partners involved with police information, competently, efficiently and lawfully carry out their responsibilities.

Implementation of the strategy will focus on the following:

- Customer-focused Service Delivery;
- Governance;
- Lawful Use of appropriate information;
- Effective use of appropriate information;
- Information as an SPSA asset;
- Information as a shared resource;
- Infrastructure management of information;
- Strategic management of information.

This IMS is not a stand alone document. It is intrinsic to how SPSA manages all of its information within the policing context and as such informs, and is informed by, all other SPSA policies. By its very nature, the management of all police information will form part of SPSA's usual business; be integrated and consistent across all business areas within the SPSA; and be reviewed and updated in line with other SPSA policies.

This strategy does not take a systems approach but will ensure that information is managed across all SPSA objectives, functions and processes in accordance with MoPI CoP.

2 Strategic Aim

The Scottish Police Services Authority's vision for Information Management is to:

Provide the best possible service to our customers by providing reliable information at the point of need; where individuals understand the importance of using it correctly, sharing it lawfully and protecting it from improper use.

3 IMS Strategic Objectives

To achieve its aim, the SPSA will:

- Work to achieve the required standards to comply with legislation and relevant SPSA policies including MoPl CoP;
- Manage its information corporately;
- Identify and support effective practice in the management of police information across all business areas;
- Promote an SPSA-wide understanding of the information lifecycle;

- Ensure that SPSA infrastructure and processes can provide the right information to the right people at the right time for the right purpose.

To achieve its objectives SPSA will be guided by the following principles of information management. They reflect the fundamental information management principles of the SPSA.

4 Information Management

4.1 The Principles

SPSA is committed to the following five Information Management principles as defined by the International Standards Organisation (ISO) 15489:

- Recognise and understand all types of information;
- Understand the legal issues and execute duty of care responsibilities;
- Identify and specify business processes and procedures;
- Identify enabling technologies to support business processes and procedures;
- Monitor and audit business processes and procedures.

4.2 The Objectives

Information management cuts across all of the SPSA's business activities. It is critical that a coordinated and cohesive approach is taken to improve performance in support of the SPSA's objectives:

- Information will be managed to support business processes;
- Information will be accurate, up-to-date and readily accessible to those who have authority to see it;
- Information will only be retained where necessary;
- Information will only be lawfully disclosed or shared where necessary;
- A consistent approach to managing information will be adopted across SPSA based on the lifecycle of information in accordance with MoPI;
- Methods of information management will be secure, protected, legal, and subject to environmental and proportional cost issues.

4.3 The Standards

The following standards apply but are not exhaustive:

- ACPO/ACPOS Community Security Policy;
- HMG Information Assurance Maturity Model;
- Requirement for information to comply with the principles of the National Intelligence Model (NIM);
- Classification, grading and recording of police information;
- Storage and handling;
- Removal of unnecessary duplication;
- Quality of information;
- Evaluation;
- Audit;

- Risk management;
- Vetting.

These standards provide an opportunity for achieving national consistency within the Police community through complying with the MoPI CoP by:

- Ensuring the SPSA understands the value of information and is able to exploit it as a corporate asset;
- Providing the standards for information management in respect of definitions, data standards and the rules for disclosing/sharing;
- Integrating all SPSA policies and protocols relating to, and in the context of, managing police information;
- Putting in place cost effective mechanisms to ensure the SPSA and its partners have access to the right information, in the right form, at the right time.

4.4 Business Management

The business should ensure the following:

- Duty to obtain and manage information;
- Cost-effectiveness in information management;
- Commitment to an information culture;
- Information as a business asset - recognising the value of information used in decision making and program management.

4.5 Staff Management

Management responsibilities towards information include the following:

- Ownership of information;
- Users' responsibilities towards information;
- Competency in handling information;
- Investment in appropriate resources, skills and training.

4.6 Information Sharing

The business should ensure the following:

- Duty to share information lawfully and appropriately;
- The right information for the right person at the right time;
- Protection of sensitive information and sources;
- Obligations of those receiving information.
- Information Sharing Agreements will be available to staff in repositories on the relevant Intranets. A named individual will be nominated to manage the respective repository.

4.7 Data / Information Management

The business should ensure compliance with the following:

- Creation, management, retention, audit, review and disposal of information;
- Conformity and compliance with external records and requirements;
- Use of appropriate information technology;
- Security of information;
- Aggregating data;
- Storage of information;
- Information life cycle;
- Data Protection Act 1998;
- Freedom of Information (Scotland) Act 2002.[1]

5 Scope of Strategy

This strategy mandates the areas that are identified under MoPI CoP and should be used as good practice for all other information management responsibilities.

It applies to all information received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff employed by the SPSA in the course of carrying out their duties. This document covers all formats of information including electronic and hard copy.

This strategy does not redefine organisational structures, nor determine technology-based solutions; however, it will inform future technical developments.

6 Responsibilities

The person with overall responsibility for this strategy is the SPSA Chief Executive

The SPSA has a corporate responsibility to manage all information created, received and held in accordance with the regulatory environment and in relation to personal data created, received and held by the SCDEA, the SCDEA Director General.

The Police, Public Order and Criminal Justice (Scotland) Act 2006 confers on the SCDEA responsibility for information sharing powers, (S19 and S20), under the direction of the Director General, SCDEA.

[1] SCDEA is not covered by the provisions of Freedom of Information (Scotland) Act. and is under no obligation to respond to Freedom of Information requests.

The SPSA has a corporate responsibility to ensure it has a business continuity plan in place to safeguard its corporate and information assets.

The person(s) responsible for information management in the SPSA will:

- Ensure that the IMS is available for all staff, partners and the public to view;
- Give guidance for good information management practice and will promote compliance with this strategy so that all information, including police information, will be:

  accessed easily, appropriately and in a timely manner;

  for police information, processed for a policing purpose;

  shared and disclosed lawfully.
- Ensure the confidentiality, integrity and availability of the information.

All individuals within the SPSA will ensure that all information created, received and held for which they are responsible, is accurate, relevant and kept up to date, and that decisions are properly recorded, thereby ensuring accountability with an accurate audit trail.

7 Relationship with Existing Policies

This strategy has been drawn up within the context of:

- MoPI (CoP)
- MoPI Guidance
- MoPl Threshold Standards
- SPSA Records Management Policy
- SPSA Information Security Policy
- SPSA Freedom of Information Policy
- SPSA Data Protection Policy
- SPSA Retention Schedule
- Scottish Crime and Drug Enforcement Agency (SCDEA) Retention Schedule
- ACPO/ACPOS Community Security Policy

and links with other legislation, statute and common law, regulations, national and local policies and procedures affecting the SPSA.

All relevant, future policies and procedures will be written with due regard to this strategy.

The SPSA ICT Strategy is intrinsically linked to this strategy.

8 Information in the Policing Context

Information will be managed corporately and will have common standards applied to it in order for it to be used for a policing purpose. This will enable the SPSA to agree solutions to information management issues locally and nationally.

SPSA policies, procedures and working practices for all key elements of information management will comply with MoPI CoP and other relevant legislative regulations, policies and standards affecting the management of information functions across all SPSA business areas.

Good practice dictates that systems will be integrated and information received or collected will be entered into the system once as part of the operational process at the point of service delivery, without intervening manual processes.

9 Strategic and Operational Information Management

Implementation of information management practices will focus on the following the following key focus areas below.

9.1 Customer-focused Service Delivery

The SPSA will implement integrated information management processes across all business areas and activities to enable it to bring about increasingly responsive services to its customers.

9.2 Governance

The SPSA has a duty to obtain, create, manage and dispose of information needed for police purposes.

The SPSA will manage its information with due regard to the different types of information it is legislatively bound to hold, in particular information that has regulatory constraints upon its publication and that which is for internal use only.

Information will be held where and when it is considered that it is necessary for a police purpose or in support of a policing purpose and assessed for reliability.

Information originally created or recorded for police purposes will be reviewed in line with MoPI Guidance and be compliant with the principles of Data Protection Act 1998 and SPSA and SCDEA retention schedules.

When it is reviewed, information originally created or recorded for police purposes will be considered for retention or disposal.

Where appropriate and with the necessary authority the SPSA and SCDEA will delete the information if:

a) the information has been shown to be inaccurate, in ways which cannot be dealt with by amending the record; or

b) it is no longer considered that the information is necessary for police purposes or in support of a policing purpose.

SPSA is committed to improving and maintaining a fit for purpose flow of information, central to its ability to function effectively and efficiently, and to ensuring that staff is aware of the SPSA's key aims, objectives, strategies and developments.

9.3 Effective and Lawful Use of Appropriate Information

The SPSA is committed to continual development of information processes to enable effective information sharing partnerships, and ensure disclosure and dissemination in a lawful manner.

The SPSA is committed to providing an environment to support staff in their role of managing the lifecycle of the information.

Where appropriate, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information will be recorded to permit later review, reassessment and audit.

The format in which the information is recorded will comply with standards agreed and applied across the police service to facilitate exchange of information.

9.4 Information Risk Management (IRM)

IRM is owned by the Senior Information Risk Owner (SIRO)[2] on behalf of the Chief Officer Group/Team[3] and should form part of its overall responsibilities in the governance of risk.

Information risk management should be recognised as the responsibility of everyone in the organisation. Management teams should develop a culture to encourage behaviours that ensure information is valued, protected, used for the public good and in accordance with applicable legislation.

9.5 Risk Appetite

IRM requires the identification of the Information Risk Appetite[4] of the organisation - set the levels of risk the organisation is prepared to accept in pursuit of its business objectives.

The Information Risk Appetite will determine the organisation's risk tolerance to individual information systems, projects or programmes and enable the delegation of risk management decisions and responsibilities with clear thresholds to specified functions.

9.6 Risk Registers

IIRM requires the reporting and recording of Information Risks on a Risk Register. This will ensure that risks are monitored and managed at the appropriate level in the organisation. Where Information risks are held on a Corporate Risk Register they should be easily identified as information risks for traceability purposes and alignment to the evidential requirements of the HMG Information Assurance Maturity Model (IAMM).

The levels at which risks are owned and managed within the organisation may vary, for example a particular risk may impact one part of the organisation, such as a department, a business unit, business programme or project, or may be shared across a separate department and business unit. Therefore risks may appear on more than one risk register.

---

[2] The SIRO in police forces is usually designated to the Deputy Chief Constable or equivalent.

[3] The Chief Officer Group/Team in police forces is headed by the Chief Constable and other Chief Officers and Police Staff equivalents. In other organisations this will be the Chief Executive Officer and their board members.

[4] Further guidance on Risk Appetite is available in the ACPO/ACPOS Information Risk Appetite and Risk Balance Case Guidance document produced by NPIA on behalf of ACPO/ACPOS.

9.7 Reporting and Monitoring Risks

An IRM framework also provides those individual functions involved with clearly defined reporting and escalation paths within the organisation to ensure information risks can be addressed with the appropriate level of senior management support and involvement.

9.8 Shared Risks

An important aspect of IRM particularly for the police community is to recognise information risks and to be able to articulate them to its partner organisations. This ability to communicate risks will raise awareness of potential, owned and/or shared risks and the impacts on the wider community (e.g. other forces and agencies, the Criminal Justice Community, NHS, Social Services, etc).

To facilitate this SPSA should agree with its partners, how it will manage and communicate these risks to an agreed format. This will ensure risks can be managed by the appropriate owners and enable each organisation to discharge its responsibilities appropriately. For information risks which are jointly owned, the organisations should consider recording them on their respective corporate risk registers.

9.9 Information as an SPSA Asset

Each SPSA business area will have a defined business process owner who will be responsible for the information's lifecycle processes.

All information will have a defined custodian who will be responsible for its management and for making it accessible to those who need it in a secure and timely manner under central guidance.

The SPSA will maintain and develop the quality of facilities and equipment relevant to information provision.

9.10 Information Asset Register (IAR)

To facilitate IRM and for it to be effective it is necessary to know what information assets of value an organisation has. This is particularly relevant when establishing the business harm that can be caused by inappropriate use or unauthorised disclosure.

In the context of this IMS an information asset register[5] should detail all information assets (including those in paper record systems and IT networks/services) and briefly describe the asset, its protective marking, who owns or is responsible for the asset **(commonly known** as the Information Asset Owner) and any other information of relevance as determined by the organisation. The IAR should have an effective process to maintain its accuracy and should be available to staff.

9.11 Information as a Shared Resource

SPSA will ensure information is accurate, reliable and up-to-date, and available to Police Forces and Agencies as specified in the MoPI CoP requiring information for police purposes.

[5] See HMG IA Standard 6 Protecting Personal Data and Managing Risk.

The SPSA will have in place appropriate protocols for sharing information.

Procedures will be applied to a request for access to information recorded for police purposes, in particular, where it is necessary to protect the source of sensitive information or the procedures used to obtain it.

In making national and local agreements and protocols for the sharing of police information with persons or bodies other than Police Forces where a power to share exists, or in responding to individual requests for information outside such agreements or protocols, the Chief Executive will require those to whom information is made available, to comply with the following obligations:

a) A formal information sharing agreement will be required to be signed by the partners

b) Police information made available in response to such a request will be used only for the purpose for which the request was made;

c) If other information available, at the time or later, to the person or body requesting police information indicates that police information is inaccurate or incomplete, they will at the earliest possible opportunity inform SPSA of such inaccuracy or incompleteness, either directly or by reporting the details to the relevant Business Process/System Owner (BPO). The BPO responsible for the police information concerned will then consider, and if necessary, record any additions or changes to the recorded police information.

10 Infrastructure and Strategic Management of Information

SPSA is committed to a consistent approach to the strategic management of information at all levels, led by the relevant information management board.

The SPSA has a corporate responsibility for ensuring an appropriate information management infrastructure is implemented and maintained, including developing robust, reliable, flexible, scalable and secure systems, with cognisance of HMG Information Assurance standards and guidance, for both electronic and paper-based records/documents.

The infrastructure will host integrated systems to provide seamless access to related information across different functional systems e.g. electronic automated systems to manage time and labour intensive activities internally and externally and it will be developed to accommodate existing and emerging business processes.

Business process owners will be responsible for developing strategic liaison between departments to facilitate coherent development of information provision.

As SPSA becomes increasingly dependent on electronic information systems for its effective operation, the SPSA will ensure these systems do not suffer major periods of unavailability, and business continuity plans will be developed by business area owners in partnership and consultation with ICT, informed by realistic risk assessments.

11 Information Systems and Accreditation

Information Risk Management (IRM) is a governance framework for the SPSA to manage information risks, it requires a measurable business process that is consistent and can be replicated. This ensures the risks can be managed to a set of baseline measures and the process can be shared, risks understood by members of the organisation and partnership organisations. To enable these requirements the police service has adopted the HMG Accreditation process, which produces a Risk Managed Accreditation Document Set (RMADS) [6].

Accreditation is a mandatory business process for all Police Information Systems that hold protectively marked information. It is mandated by both the ACPO/ACPOS Information Systems Community Security Policy (CSP) and the HMG Security Policy Framework (SPF)[7].

Accreditation forms part of the overall governance of an information system in that it helps to ensure that security risks are identified, well understood and managed throughout development, in-service and decommissioning of the system. Thus Accreditation acts as the in-service life cycle management for information assurance and risk management.

The RMADS also identifies functions and responsibilities in the operating Security Procedures.

Accreditation provides an assessment that an information system meets its IA requirements and that the residual risks, in the context of the business requirement, are acceptable to the business and agreed risk appetite.

12 Information Management Functions and Responsibilities

As a matter of policy and procedure, all SPSA staff must understand their responsibilities when using or communicating personal or other data and information.

In practice, everyone working for, or with, the SPSA who receives, creates, maintains, stores, reviews, discloses/shares or disposes of information, has a common law duty of confidentiality. This responsibility is established at, and defined by, law.

In addition to individuals' responsibility for information management, there are core levels and functions that have been identified to ensure that police information and information in support of a policing purpose is managed effectively, efficiently and lawfully. Each of these has a different combination of responsibilities but some are shared.

This diagram in **Appendix A** is not intended to show a preferred hierarchy or to indicate what grade / rank should be associated to the functions described in this section or which departments the functions should be located in. It shows a possible organisational hierarchy of how some of the functions could be implemented and many other allocations of functions are possible.

[6] This process is fully described in the HMG Information Assurance Standard 1 and 2. NPIA has also produced an Accreditation Guidance document for the police community.

[7] The Security Policy Framework is mandatory for all organisations following the government protective marking scheme.

12.1 The Board

The SPSA Board will deal with strategic issues surrounding information management.

The Board will approve the organisation's policy toward information assets and thus identify how compliance with that policy will be measured and reviewed, including:

i) identification and recognition of information assets and the classification into those of value and importance that merit special attention and those that do not;

ii) quality and quantity of information for effective operation ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent;

iii) the appropriate use of information in accordance with applicable legal, regulatory, operational and ethical standards and the roles and responsibilities for the creation, safekeeping, access, change and disposal of information;

iv) the protection of information from theft, loss, unauthorised access, improper use, including information which is the property of others;

v) harnessing of information assets and their proper use for the maximum benefit of the organisation including legally protecting, licensing, re-using, combining, re-presenting, publishing and destroying;

vi) developing and maintaining a strategy for information systems, including those using computers and electronic communications and the implementation of that strategy with particular reference to the costs, benefits and risks arising;

vii) identifying and actioning the appropriateness of a central oversight role for all information held by the SPSA.

12.2 The Executive

The Chief Executive has ultimate ownership of the SPSA IMS.

As Data Controllers, the Chief Executive of SPSA and the Director General of SCDEA, in line with the Data Protection Act 1998 (DPA), as distinct data controllers, have the duty to comply with the data protection principles in relation to all personal data with respect to which he/she is the data controller, including the following:

i) determine why, as well as how, personal data including sensitive personal data, is to be processed and what security measures will be appropriate;

ii) has a duty to ensure that the collection and processing of any personal data within the SPSA complies with the data protection principles;

iii) retains full responsibility for the actions of the data processor;

iv) notifies all processing operations that involve personal data to the Information Commissioner and keeps this notification up-to-date.

The role of Data Controller is a primary legislative function. The controls for meeting the legal obligations for personal data management can be delegated as appropriate, with clearly defined responsibilities and the ability to report directly to the Data Controller as necessary.

The Chief Executive for SPSA and the Director General for SCDEA have overall executive responsibility for management and use of information within their remits.

The Chief Executive for SPSA and the Director General for SCDEA will ensure that the SPSA adopts policy, procedures and processes for the management of information, and support their application-wide so that information is used effectively for police purposes and in support of policing purposes and in support of consistent national standards.

The SPSA are Data Processors for the systems it manages on behalf of the Forces and SCDEA and formal contracts must be in place which will require compliance with the DPA and The Government's Security Policy Framework.

12.3 Accounting Officer (AO)

The AO function is usually undertaken by the Chief Constable in a police force or the Chief Executive Officer equivalent in other organisations as in SPSA. The AO has overall responsibility that information risks are assessed and mitigated to an acceptable level. This will include the completion of an Annual Statement of Internal Controls which includes a statement regarding IA controls.

12.4 The Legal and Compliance Team

The SPSA will have a Legal and Compliance Team to implement, maintain and monitor the IMS and the supporting policies, standards and guidance.

The Legal and Compliance Team will provide advice and guidance to all staff involved in the management of information through the specialism's of its members.

The Legal and Compliance Team is responsible for ensuring that the business is aware of its obligations and that relevant guidance is available for the management of police information in SPSA, such as data protection, information assurance, freedom of information, records management and information sharing.

The Legal and Compliance Team will be responsible for ensuring information management training is provided in line SPSA objectives including:

i) ensuring a training needs analysis is conducted;

ii) establishing appropriate training programmes and schedules;

iii) identifying appropriate training products.

The responsibilities of the Legal and Compliance team include the following:

a) Ensuring:

i) The strategic direction of the SPSA in all information management disciplines;

ii) SPSA processes and systems take cognisance to the MoPI CoP, Guidance and Threshold Standards;

iii) The SPSA IMS is established and maintained;

iv) All Information Sharing Agreements are MoPI compliant.

v) The SPSA policies and Standard Operating Procedures (SOPs) are appropriate to make certain that information is easily accessible, searchable and retrievable;

vi) The SPSA meets national requirements for the management of police information;

vii) Compliance with the ACPO/ACPOS Community Security Policy (CSP);

viii) Security Operating Procedures (SyOps) for all SPSA systems are available to relevant staff;

ix) Reporting lines exist to allow Department Heads to raise issues to SPSA Compliance Team if necessary;

x) Reporting lines exist to allow the Compliance Team to discuss matters (their own or those raised by Department Heads) at an ACPOS level where appropriate;

xi) Appropriate role/function is available to represent the SPSA at named forums.

b) Overseeing:

i) Management of Subject Access Requests under the Data Protection Act 1998.

ii) Management of Freedom of Information (including compliance with the ACPOS Freedom of Information Manual) under the Freedom of Information (Scotland) Act 2002;

iii) Compliance with the ACPOS CSP;

iv) Compliance with the SPSA and SCDEA Retention Schedules.

c) Supporting staff to share information appropriately.

d) Contribute to the development of Information Sharing Agreements.

e) Liaising with Department Heads when necessary to provide guidance and support on Information Management.

f) The Legal and Compliance Manager is responsible for overseeing the delivery of an Information Assurance framework across the organisation, ensuring compliance with relevant policies, procedures and legislation. Information Assurance encompasses Information Security, Data Protection, Freedom of Information and Records Management.

12.5 Senior Information Risk Owner (SIRO)

In accordance with HMG Information Security Standard 6 *"Protecting Personal Data and Managing Information Risk"* October 2008 V1.0 and to comply with the ACPO/ACPOS Community Security Policy and HMG Security Policy Framework, SPSA must name a board member as "Senior Information Risk Owner" (SIRO). The term SIRO is only used for the single individual within each organisation with ownership of the corporate information risks and leading the organisation's response. The SIRO is an executive who is familiar with information risks and the organisation's response. The SIRO may also be the Chief Information Officer (CIO) if the latter is on the board. They own the information risk policy and risk assessment, act as an advocate for information risk on the board and in internal discussions, and provide written advice to the accounting officer on the content of their Statement of Internal Control relating to information risk.

The SIRO has responsibility for understanding how the strategic business goals of the SPSA may be impacted by information management systems failure. The SIRO is directly responsible for ensuring that information risk management and management processes are established and adhered to SPSA-wide. This is a strategic responsibility, which will not be confined to information technology or information governance departments.

The SIRO has responsibility to determine and set the Information Risk Appetite level[8] in an organisation and is the final decision maker for accepting risks outside the level of acceptance for the specific roles listed later in this document[9].

The SPSA's SIRO[10] is the Director of Strategy and the SCDEA's SIRO is the SCDEA Director General.

Further detail on the SIRO role is provided in the table[11] below:

Aspect of role	**Supporting actions**
Lead and foster a culture that values, protects and uses information for the public good	• ensures the organisation has a plan to achieve and monitor the right culture, across the 0rganisation and its partners • takes visible steps to support and participate in that plan (including completing own training) • ensures the has Information Asset Owners[12] who are skilled, focussed on the issues, and supported, plus the specialists that it needs

[8] Information Risk Appetite is seen as an essential element of the Information Risk Management process and sets out the organisation's willingness to tolerate a particular level of exposure to risk or set of risks and provides a framework for the organisation to operate within, in terms of what is and what is not acceptable to the organisation.

The Information Risk Appetite and associate Tolerance levels will provide Accreditors and those with responsibility for or involved with information risk activities with a robust framework within which to make accreditation and risk management decisions, and know when to escalate risk to the Information Risk Owner (IRO) and SIRO.

[9] Some risks captured through Accreditation, Information Asset Owner returns, or from other sources will be escalated to the SIRO for a risk management decision, through a Risk Balance Case). This is generally due to those risks being deemed to be above the level of acceptance for the specific roles and accountability, which cannot be accepted lower down the information risk management chain. This maybe due to the likelihood of occurrence is sufficiently high, the potential impact is very high, or the information system itself is particularly sensitive (making the appetite to risk particularly low or more averse).

[10] The SIRO in police forces is usually designated to the Deputy Chief Constable or equivalent.

[11] Reference: HMG. Security Policy Framework. V3.0. Oct., 2009

[12] **Information Asset Owners** are senior individuals involved in running the relevant business. Their role is 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 the public good, and provide written input to the SIRO annually on the security and use of their asset.

Lead and foster a culture that values, protects and uses information for the public good	• ensures the organisation has a plan to achieve and monitor the right culture, across the 0rganisation and its partners • takes visible steps to support and participate in that plan (including completing own training) • ensures the has Information Asset Owners[13] who are skilled, focussed on the issues, and supported, plus the specialists that it needs
Owns the overall information risk policy and risk assessment process, test its outcome, and ensure it is used	• ensures that risk policy is complete – covering how the organisation implements at least the minimum mandatory measures in own activity and that of delivery partners, and how compliance will be monitored • ensures that risk assessment is completed at least quarterly taking account of extant Government-wide guidance (available from Cabinet Office) • receives six monthly report from the Accreditor on the assurance of the organisational Information Systems • based on the risk assessment, understands what information risks there are to the organisation through its delivery chain, and ensures that they are addressed, and that they inform investment decisions • ensures that risk assessment and actions taken benefit from an adequate level of independent scrutiny

[13] **Information Asset Owners** are senior individuals involved in running the relevant business. Their role is 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 the public good, and provide written input to the SIRO annually on the security and use of their asset.

Advise the accounting officer on the information risk aspects of his statement on internal control	• receives annual assessment of performance, including material from the Information Asset Owners and specialists, covering minimum mandatory measures as well as actions planned for the department's own circumstances • provide advice to Accounting Officer on the information risk parts of their statement on internal control • shares assessment and supporting material with relevant Government Departments, to support cross-Government work

12.6 Information Asset Owner

This function is further defined in *HMG Information Security Standard nos. 2 and 6*. The Information Asset Owner is usually a senior officer or member of staff involved in running of a business area within the organisation. Information Asset Owners act as the custodian for live data, ensuring their information asset(s) and associated risks are effectively managed.

As part of their review of information risk, Information Asset Owners are responsible for ensuring the information assets assigned to them have current accreditation, and undergo re-accreditation within an appropriate time frame. They should also be involved in the procurement processes for any new information systems involving the information assets they have responsibility for.

The Information Asset Owner needs to have a full understanding of the information asset and how it is used. This will assist them to recognise and manage any risks to their information assets. They are expected to report quarterly or at least annually to the SIRO on any security issues or risk and the use of the information asset.

12.7 Information Risk Owner (IRO)

The IRO is usually a member of the Chief Officer Team/Board or senior officer who has delegated authority from the SIRO.

The IRO has responsibility for ensuring information risk management is effectively discharged within their area of responsibility. This includes ensuring there is sufficient budget and skilled personnel to address information risk. They are also accountable for ensuring their capabilities (Systems/Services) are accredited.

The IRO should own the IA risk register and should engage with the relevant IAOs to understand and agree the risks to information used in their area of responsibility. They are also required to make management decisions with regards to information risks and to outline plans for mitigating or accepting risks on behalf of the SIRO.

An IRO may also have Senior Responsible Officer (SRO) responsibilities for large organisational projects or programmes.

12.8 Senior Responsible Officer (SRO) – Projects / Programmes

The SRO is responsible for managing business and information risks for specific projects or programmes. They are responsible for ensuring information risk management processes are followed within a project or programme on behalf of the SIRO and board level business owners.

The SRO cannot assume ownership of any corporate risks that are incurred outside of the scope of their particular project or programme.

12.9 Senior Systems Owner (SSO) / System Owner (SO)

These two functions are described in the MOPI Guidance - Threshold Standards and also in the ACPO Data Protection Manual of Guidance.

These titles maybe given to those personnel responsible for specific information systems, through the life cycle of those systems - from project stage, through to operational live environment and to the decommissioning of the information systems.

These functions will typically be involved in data quality and ensuring risk management processes are carried out in respect of the information systems they are responsible for.

The SSO/SO may have a similar function to the IAO and SRO, but they will not usually own an information asset or own a business area, but would own an individual or series of information systems within a business area.

12.10 Information Asset Administrator (IAA)

This function may be appointed by the Information Asset Owner where additional support is required for an asset. However the responsibility still lies with the Information Asset Owner and cannot be delegated to the IAA. The IAA may for example manage user access for a particular information system in line with the system accreditation requirements and produce reports on system usage for the IAO.

This function should not be confused with **System Administrators**, who are generally more involved with the technical aspects of information systems and applications e.g. installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other computer issues/problems.

12.11 Accreditor

The role of the Accreditor is to act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the Board. Although it is necessary for the Accreditor to have an understanding of ICT related technology, the role does not require a deep technical knowledge. Indeed, it is necessary for the Accreditor to step back from the technical detail and consider risk management in the round to ensure the physical, personal, procedural and technical controls are balanced. It is important, therefore, that the Accreditor has access to people who have a professional technical understanding of the technologies involved, to support the accreditation process. To support this requirement funding should be identified at the outset for any specialist technical advice and services such as Technical and IA Consultants, IT Health Checks and assurance services. Accreditors are accountable for their decisions and actions in their role as information assurance risk assessors and risk managers.

The Information Assurance Officers within the SPSA Legal and Compliance Team take on the role of local accreditor within the relevant part of the SPSA. The local accreditors liaise with the National Accreditor for Police Systems at the National Police Improvement Agency (NPIA).

12.12 Information Assurance Officer / Senior Compliance Officer

The SPSA Senior Compliance Officer has line management responsibilities for the Information Assurance Officers and Record Manager(s).

The Senior/IAOs have various responsibilities with regard to the development and implementation of the Information Security Policy and procedures within their areas of responsibility. Their responsibilities towards Accreditation may include implementation of the Risk Treatment Plans and through-life IA measures reporting on risks to the organisation where there is non compliance of standards, policy or procedures.

The Senior/IAOs may also have other functions or responsibilities that are essential to the IA of the organisation, such as an advisory function to the organisation on IA matters, personnel security or physical security. In some instances the IAOs and the Accreditor function are combined. They may also have other functions e.g. Data Protection Officer.

The IAOs are usually the central contact between the SPSA / specific business area, the police community and national bodies on matters relating to information assurance e.g. the National Accreditor for the Police Service (NAPS) at NPIA or with CESG.

The SPSA Senior Compliance Officer and the Information Assurance Officers are appointed in line with the CSP, which specifies the officers responsibilities including;

i) acting as the point of contact for all information security issues;

ii) implementing organisational structures, policies, procedures and risk management programmes with respect to security matters;

iii) providing advice on the correct and secure operation of information processing systems and applications;

iv) ensuring appropriate security measures are in place for procedures and technical measures to prevent unauthorised or accidental access to, amendment of, or loss of police information;

v) quality assuring local information security policy documentation;

vi) demonstrating an approach to implementing security that is consistent with national and local requirements;

vii) marketing the need for information security;

viii) providing advice on security education and training;

ix) co-ordinating all investigative and reporting action that may be undertaken into actual and suspected incidents of security significance;

x) co-ordinating and advising on the implementation of specific security requirements for new and legacy systems and services;

xi) establishing and ensuring that third party agencies sharing, accessing, storing or processing information and information assets owned by the SPSA, comply with the defined threshold standards;

xii) maintaining appropriate contacts with other community members, Government departments and regulatory bodies;

xiii) liaising with Department Heads when necessary to provide guidance and support on information security matters;

xiiii) representing SPSA interests at a Regional and National level on information security issues;

xv) ensuring appropriate security measures are afforded to information, including personal data, thereby assisting SPSA' compliance with the DPA in order to discharge security responsibilities;

xvi) liaising on all Information Security matters between the SPSA and relevant regional or national bodies (including the ACPOS Information Security Group).

12.13 IT Security Officer (ITSO)

The ITSO function is responsible for the security of information in electronic form. They are responsible for ensuring that IT security is implemented effectively and co-ordinating the technical aspects of protective monitoring. The ITSO function may also include the provision of security technical support and support in the development of Risk Management Accreditation Document Set (RMADS) for systems that have to undergo accreditation.

The ITSO function can be regarded as an individual function specialising in the technical aspects of security or it could be a combined function with a suitably qualified IA or IT specialist within the organisation.

Within SPSA the ITSO function is carried out by the Technical Security Manager.

12.14 Crypto Custodian

The main responsibilities of a Crypto-Custodian are:

- Ensuring compliance with HMG and departmental policy and procedures governing CRYPTO/ACCSEC[14]/Crypto Controlled Items (CCI) items.
- Management and accounting of all CRYPTO/ACCSEC/CCI items under their control.
- Emergency action in accordance with HMG and/or departmental instructions.
- Comsec incident reporting (to the Comsec Officer and CINRAS) and, where appropriate, investigation and recovery. *(Detailed responsibilities are contained in separate HMG Policy.)*
- A *Deputy Custodian* must be appointed to deputise for the Custodian during periods of absence, at which times he/she will assume the duties outlined above.
- Ideally the Deputy Custodian should also be the witnessing officer for destruction and musters, where applicable, as a means of maintaining awareness of their responsibilities.

12.15 Records Manager

SPSA will have a designated Records Manager(s) (RM). The RM's responsibilities include:

i) provide a single point of contact to process owners;

ii) ensure that the records management policy and standards are kept up-to-date and relevant to the needs and obligations of the SPSA, through consultation and assessment against external standards;

iii) ensure review, retention and disposal schedules are implemented;

---

[14] An asset with a caveat of ACCSEC means **Acc**ountable **Sec**urity. As a minimum you must know where the asset is located and it must be secure at all times.

iv) conduct local quarterly review and evaluation of their systems registers to ensure accuracy and completeness;

v) ensure that all files are available for those with authorised access;

vi) determine records management relationships with internal and external stakeholders, including audit and management teams;

vii) ensure that management teams supervising divisional/department records management have the necessary skills and competencies;

viii) manage the storage conditions of all records on-site and off-site including contract storage services;

ix) monitor individual and SPSA compliance with the records management policy and standards.

x) ensuring that information management policies and procedures are being communicated to appropriate personnel and are being adhered to;

xi) monitoring use of shared/personal storage space;

xii) ensuring that metadata exists for all documents and files;

xii) monitoring the use of the SPSA file management systems and processes, including appropriate naming and assigning of metadata for all documents and folders;

xiv) ensuring that appropriate data standards and targets are in place and met;

xv) ensuring that appropriate paper filing takes place;

xvi) ensuring that the accuracy of data is regularly assessed.

12.16 Data Protection Officer

The SPSA Information Assurance Officers carry out the Data Protection Officer's (DPO) role within the relevant parts of the SPSA.

The DPO's responsibilities include:

i) managing the Data Controller's statutory obligations in respect of the Data Protection Act 1998 (DPA) including; notification of processing to the Information Commissioner; compliance with the Data Protection Principles and securing individuals rights under the Act, including subject access requests;

ii) maintaining an up to date knowledge of, and advising on relevant legislation and general developments in data protection and related matters;

iii) promoting awareness of data protection matters through training, policy development, advice and guidance;

iv) undertaking systematic auditing and monitoring of information and systems in accordance with the ACPO/ACPOS Data Protection Audit Manual, including risk assessed strategic audit plans;

v) ensuring information and systems comply with the relevant legislation including the DPA;

vi) ensuring that appropriate security arrangements exist to protect information, including where necessary that suitable contracts are drawn up relating to the processing of police information by third parties;

vii) investigating and resolving complaints made in relation to the handling of personal information (in relation to data protection);

viii) assisting where appropriate in the investigation of disciplinary and criminal matters relating to data protection;

ix) liaising on all data protection matters between the SPSA/SCDEA and relevant regional or national bodies (including the ACPOS Data Protection Officer's Group and the Information Commissioner's Office);

x) liaising with Department Heads when necessary to provide guidance and support on data protection matters;

xi) ensuring that the ACPO/ACPOS Manual of Guidance on Data Protection are disseminated and adhered to SPSA-wide;

xii) liaise directly with the SIRO;

xiii) liaising regularly with the SPSA's Records Manager(s).

12.17 Freedom of Information Officer

The SPSA Legal and Compliance Team carry out the Freedom of Information Officer's role within the relevant parts of the SPSA.

A Freedom of Information Officer's responsibilities include:

i) managing the SPSA obligations in respect of the Freedom of Information (Scotland) Act 2002 (F0ISA) including the SPSA publication scheme and requests for information under the Act;

ii) maintaining an up to date knowledge of, and advising on relevant legislation and general developments in freedom of information and related matters;

iii) ensuring that the ACPOS Freedom of Information (Scotland) Act 2002 Manual of Guidance is disseminated and adhered to SPSA-wide;

iv) promoting awareness of freedom of information matters through training, policy development, advice and guidance;

v) liaising with Branch Command Unit/Department Heads when necessary to provide guidance and support on freedom of information matters;

vi) liaising on all FOl matters between the SPSA and relevant regional or national bodies (including the ACPOS Data Protection and Freedom of Information Portfolio Groups and the Scottish Information Commissioner's Office).

12.18 Vetting Officer

The SPSA has a dedicated Vetting Officer who is responsible for the coordination of all vetting within the SPSA covering all SPSA personnel, contractos and temporary staff in line with the ACPO/ACPOS Vetting Policy and HMG standards for Government vetting, as appropriate for specific job roles.

12.19 Disclosure Officers

Within the SCDEA nominated staff carry out the role of Disclosure Officers. Their responsibilities include:

i) all requests for, and disclosure/sharing of, information are carried out in accordance with SCDEA / ACPOS ISAs and with due regard to all relevant legislation and guidance.

ii) all information received is conveyed, handled and kept in a confidential and secure way and, if not disposed of, returned to the originating agency when it is no longer required;

12.20 Chief Information Officer (CIO)

The Chief Information Officer (CIO), or Information and Communications Technology (ICT) Director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO typically reports to the chief executive officer and is responsible for all Information Technology functions within the enterprise providing ICT leadership, driving cost-effective operations but long-term strategic success.

In brief the CIO directs and manages computing and information technology strategic plans, policies, programs and schedules for business and finance data processing, computer services, network communications, and management information services to accomplish corporate goals and objectives.

12.21 Branch Commander unit / Department Heads

The responsibilities of a Branch Commander Unit / Department Heads with regards to information management include:

i) ensuring the area or department under their management complies with all relevant policies, procedures and processes relevant to information management;

ii) ensuring the area or department under their management complies with all legislation relevant to information management;

iii) ensuring the area or department under their management complies with the MoPI CoP, Guidance and Threshold Standards;

iv) liaising with the Records Manager, Data Protection Officers, Freedom of Information Officers and Information Assurance Officers where necessary to seek advice and to ensure information is shared appropriately within the boundaries of the SPSA and national policy and legal framework;

v) ensuring data quality is treated as a priority;

vi) ensuring staff are recording information on the appropriate format;

vii) ensuring staff responsible for recording, and undertaking reviews of, police information are trained in accordance with the MoPI National Training and Delivery Strategy.

12.22 Users of Information Assets

All users have to accept a level of responsibility for information risk ownership when using the organisation's ICT systems or services. However, it is the responsibility of the SIRO and those with delegated responsibility for IA to ensure all users are aware of the risks and that they formally acknowledge their acceptance of the corporate security policies and user guidance specific to the system or service they are using.

12.23 Staff

All staff involved in the management of police information or who have access to personal data have individual responsibilities as detailed below:

i) to apply the basic principles of effective information management (as contained within the MoPI CoP and Guidance) including the application of consistent processes and decisions, 'owning' decisions and working as part of a team in a system with many interdependent links;

ii) to recognise the value of trust, confidentiality and information security and the dangers of inappropriate sharing of police information;

iii) to recognise the value of sharing and disclosing information and the dangers of failure to share when the circumstances require it;

iv) to be familiar with, and adhere to, SPSA policy, SOPs and processes when managing information;

v) to be aware of the current intelligence requirements; to ensure that information is collected for a policing purpose;

vi) to record information in the appropriate format;

vii) to adhere to data standards;

viii) to disseminate information where appropriate;

ix) to continuously apply standards for data quality, consistent and accurate recording;

x) to apply operating rules relevant to business areas to which they have access;

xi) to apply rules relating to information security including applying protective marking to information under the Government Protective Marking Scheme (GPMS).

xi) where applicable conduct a risk assessment where the sharing is carried out with the partners in the voluntary, public or private sectors who do not have a statutory purpose to share information;

xii) will only share in accordance with agreed procedures;

xiii) to ensure compliance with all relevant legislation including the Human Rights Act 1998, Data Protection Act 1998 and Freedom of Information (Scotland) Act 2002.

All staff responsible for creating records will:

i) ensure person records are unique;

ii) quality assure the recording of the 5x5x5 and ensure the linking together of information where relevant; to identify opportunities for analysis of series or linked events;

iii) comply with the SPSA and SCDEA retention schedules and enter the review date for a record at the point of creation where possible;

iv) apply provenance to the information recorded; to apply relevant priority assessment if appropriate.

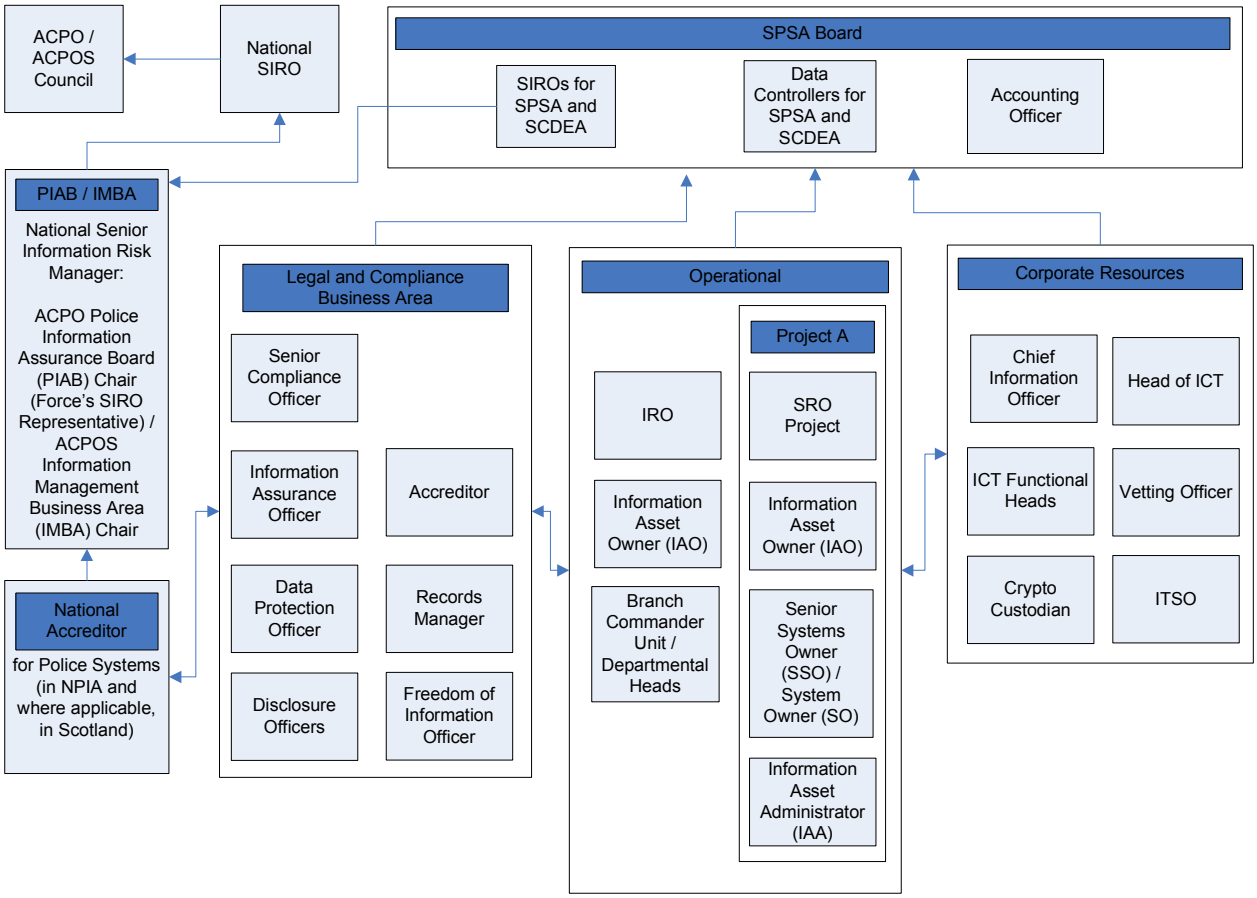
All staff responsible for reviewing records will:

i) follow the SPSA and SCDEA Retention Schedules reviewing records to determine their continued necessity for a policing purpose;

ii) document the review process wherever there is no automated mechanism in place; and

iii) ensure that information to be disposed of is not duplicated, and therefore retained, elsewhere.

13 Appendix A – Functional Information Management Roles



14 Glossary

Data Information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68. (Data Protection Act 1998), or is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d) (this fifth category was created by the Freedom of Information Act 2000 with effect from 01 January 2005).

The component(s) of information such as numbers, words or pictures without context, which in themselves - without any context - mean little and say even less. Data becomes information once it is put into a framework or structure that provides context.

Document A structured unit of recorded information, published or unpublished, in hard copy or electronic form, and managed as a discrete unit. (ISO 15489:2001) A document forms part of a business transaction and is linked to other documents relating to that transaction or process.

Information Data that has context and meaning and is, therefore, able to be understood by people.

Information asset A definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation, i.e. they are not easily replaceable without cost, skill, time, resources or a combination. The information which comprises an Information Asset, may be little more than a prospect name and address file; or it may be the plans for the release of the latest in a range of products to compete with competitors.

It is the purpose of information security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of information assets. (Information Security Glossary: http:llwww.yourwindow.to/informationsecurity!)

Information lifecycle The creation, acquisition, cataloging/identification, storage and preservation of, and access to, information.

Information management The function of managing the organisation's information as an asset, i.e. the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making. This comprises the ability to know what information exists regarding a particular subject, where and how they are stored, ownership, and when they should be disposed of.

Metadata Descriptive and technical documentation to enable the system and the records (that are described) to be understood and to be operated efficiently, and to provide an administrative context for the effective management of the records.

Record Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. (ISO 15489: 2001)

Records management Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including

processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (ISO 15489: 2001)

15 Compliance

15.1 Diversity

There is no adverse impact on any group in terms of race, religion, gender, sexuality, disability or age in relation to this procedure. The application of this policy/procedure will be monitored to ensure compliance with the organisation's Equality and Diversity Strategy.

15.2 Health & Safety

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

15.3 Communication

This policy/procedure is available to all SCDEA staff via the Intranet. The SCDEA Governance Board is responsible for ensuring that staff are made aware of the policy/procedure and their responsibilities arising from its operation.

15.4 Monitoring and Review

This policy/procedure will be reviewed annually by the document owner.