Information Asset Owners Policy (Surrey and Sussex) (1239/2024)

Abstract

This policy details how Surrey Police and Sussex Police will create and maintain the ownership of their information assets. Also includes procedure that must be followed by an Information Asset Owner in their implementation of an information asset.

Policy

1. Introduction

1.1 This policy is required to ensure that the Surrey Police and Sussex Police (hereafter referred to as the Forces) have an up-to-date information asset registry and sets out the nature and primary responsibilities of an Information Asset Owner (IAO) in managing the risks to personal information and business critical information held within a department.

2. Scope

2.1 The essential aspect is proper control over the integrity and availability of personal and business critical information. The information must be of sufficient quality to fulfil its business function and it must be available when needed. This includes the necessity of being able to trace changes to personal and business critical information. Proper version control over information, including assets such as back-up or archive media and paper records is essential.

3. Policy Statement

3.1 An IAO is responsible for the protection of information held on Cloud and IT networks and manages other assets such as paper records and backup tapes. The IAO is also responsible for ensuring that information held is of sufficient quality and accuracy to serve the purpose for which it is processed. Critically, IAO responsibilities must also consider organisational culture and behaviours.

Procedure

1. Introduction

1.1 Information has never been more important to the essential working of policing. As the quantity, diversity, and nature of police information changes, so will the threats and vulnerabilities it faces.

2. Information Asset Owner (IAO) Role

2.1 The role of the IAO was created to provide a senior role responsible for ensuring specific information assets are handled and managed appropriately. An IAO is appointed by and reports to, the Senior Information Risk Owner (SIRO).

2.2 IAOs are senior police officers and police staff involved in running an operational or business area which uses a Surrey Police / Sussex Police or Joint Forces Information System. Their role is to understand:

• what information is held and the quality of that information.

• what is added and what is removed.

• how information is moved.

• who has access and why.

3. What is an asset?

3.1 An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively. Information assets have recognisable and manageable value, risk, content, and life cycles.

An asset has been defined for this process as a system that contains, stores, or shares personal data. System should be defined broadly and whilst the majority of the assets will be IT or cloud-based, it includes traditional filing systems.

3.2 An IAO is the person with the responsibility for the asset, this must be a senior individual involved in running the relevant part of the business; they do not necessarily have to be a regular user. The IAO is a key decision maker in relation to the business area that an information system serves, rather than the technical structure that supports the system.

3.3 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 can 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.

3.4 The IAO is the single authority owning technical systems therefore they should take full responsibility for the Force owned data held into the assets.

3.5 An asset owner can assign an Information Asset Assistant (IAA), generally an everyday user with in-depth knowledge of the system and that would be able to provide additional details. It is often the administrator who completes the annual return for assets and the owners provides the sign off on the completed product.

4. What is the asset process?

4.1 The IAO has to be appointed at the procurement and development stage of the asset and have the necessary knowledge in place about how the system will process the personal and operational data processed within it.

The IAO is accountable to the Joint Force Senior Information Risk Owner (SIRO). They must be able to demonstrate to the SIRO full Data Protection compliance for their asset.

This includes demonstrating that appropriate security measures and business continuity plans are in place.

The IAO must ensure that the Information Asset has appropriate accreditation. They must also work with the Procurement Team to ensure the Information Assets are defined correctly and the necessary security measures are in place.

4.2 The IAO has the responsibility of ensuring that the relevant Data Protection Impact Assessments (DPIAs) and Information Sharing Agreements (ISA) are conducted and signed off prior to the system being in use.

4.3 The asset process is about gathering information for the register and ensuring that the information is up to date. The Force requires the IAO to assign the IAA, and then ask them to fill out the information on our surveys which is the information that builds into the register. The respective Information Management Team keeps a copy of the survey which holds all the detail.

4.4 The Force also requires a data flow to be created (an example of data flow document is available on the intranet), to show the lifecycle of the data contained in the asset. The relevant information is put onto the Information Asset Register. Currently the Asset Register contains information about all assets across Surrey Police and Sussex Police. For further information on what the Asset Register contains please review Asset Register Information.

4.5 Keeping the Asset Register up to date will ensure compliance across both Forces with Data Protection Legislation, as well as ensuring that our information is fully understood, shared, protected, and exploited effectively.

4.6 Following undertaking the annual Information Asset Review, the IAO must check that the asset is up to date, accurate and has been risk assessed, therefore must record any identified risks or issues regarding the data held into the asset on the Joint Forces Risk Management System – KETO. These risks and issues must be reported by the IAO into the Security and Information Management Board (SIMB), for the SIRO to review accordingly.

4.7 Please see the Risk Management Policy (Surrey and Sussex) (1049) for further information.

5. Training and Responsibilities

5.1 IAOs must formally review the risks to the confidentiality, integrity, and availability of their information assets. Departments must ensure that all staff with access to personal information successfully complete Information Management Refresher Training on an annual basis.

5.2 The IAO should also request from their Force’s Information Management Team the Information Asset Owner Training for themselves and their appointed IAA. This is essential in order to have the necessary knowledge in place of the asset process and their responsibilities.

5.3 The IAO must ensure:

• they have the necessary training in place and skills, resources, and authority to discharge the responsibilities and act to rectify any issues in the relevant process.

• they will take the ownership and oversight of the information that would cover into their department, whether this is sitting on a computer, a system, or a paper file. Upon appointment as IAO, the IAO must approach Information Management to complete Information Asset Owner training.

Failure to take appropriate ownership of their Information Asset(s) will result in this being reported to the relevant Force Data Protection Officer and/or the SIRO for suitable measures to be taken.

Failure to comply with Data Protection legislation can lead to the following sanctions imposed by the Information Commissioner's Office (ICO) following an investigation or audit:

- Information Notices

- Assessment Notices

- Enforcement Notices

- Monetary Penalties – The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

• the duties are distributed across posts and organisational units in an appropriate way, and they are fully co-ordinated and visible to all relevant staff (this is applicable to the assets that are being used and managed by multiple teams or departments).

• appropriate reporting chains exist to ensure that the SIRO has full visibility of the state of information asset management across their organisation.

• assurance is available that all delegated duties are properly carried out.

6. Responsibilities

6.1 In order to meet the requirements of the Security Policy Framework (SPF), IAOs:

• Must undertake and pass Information Management Owner Training on appointment and Information Management Refresher at least annually thereafter.

• Must notify their Force's Information Management Team that they are leaving the Force / changing roles and pass the details of the new IAO (best practice would be before they leave their role). If the new IAO is not named at the time of leaving / changing roles, this responsibility would fall under IAA obligations.

• Must handover to the new IAO when leaving the Force or moving to a new role, and provide the necessary details and knowledge required of the specific assets that they have been managing. If the previous IAO has changed roles and a new IAO has been appointed, the previous responsible person is still required to go back and complete a handover, even if they no longer work in that department / unit.

• Must ensure compliance with the provisions of data protection legislation in respect of the IAO's personal information assets, in accordance with the department's compliance mechanisms and policies.

• Must work effectively with the respective Force Data Protection Officer (DPO) and their Force's Information Management Team.

7. Asset Content and Data Flow

7.1 The IAO must understand the policies governing access to the information contained in the asset. The IAO should know who currently has access to your Information Asset, and who should have access, (this information can be found in the DPIA screening questions) ensuring that any access rights granted are the minimum necessary to achieve business objectives, and then removed when no longer required.

• Ensure that registers of personal data held are compiled and maintained, including records of personal data processing mandated under Article 30 of the General Data Protection Regulation (UK GDPR) and Section 61 Data Protection Act (2018).

• Approve and minimise transfers of data contained in the asset.

• Negotiate, manage, and approve ISAs on the sharing of personal information between organisations.

• Approve arrangements so that information put onto removable media is minimised and protected. For further information on removable media, please see the Surrey Police and Sussex Police Information Security Policy (722).

7.2 The IAO must approve / agree the disposal mechanisms for paper or electronic records from their asset. To do this IAOs must have oversight of an appropriate regime of department-wide arrangements for the secure disposal of electronic or paper material, which contains personal data.

7.3 The IAO must know who has access and why and ensure their use of the asset is monitored they must agree in writing that relevant access control regimes permit the business to be transacted with an acceptable level of risk of personal data contained within the asset or, if agreement cannot be given, require that an acceptable alternative approach be adopted.

7.4 The IAO must:

• Understand the organisation's policy on use of the information.

• Check that access provided is the minimum necessary to achieve the business purpose.

• Where possible, receive records of usage checks and assure themselves that they are being conducted. To do this IAOs must:

• Establish with managers an appropriate regime for the monitoring of the use made of access to personal information, electronic or otherwise.

• Establish with managers appropriate mechanisms for the IAOs to receive summary reports on the conduct and results of such monitoring. (for further guidance, refer to DPIA

Screening questions and Information Security Asset Review, or contact the relevant Force Information Management Team).

7.5 In order to understand and address risks to the asset and provide assurance to the SIRO, they must provide an annual assessment to the Information Management Officer about the security and use of the asset.

8. Unstructured Data

8.1 The IAO must take responsibility for respective business areas they lead, and information held on the Forces networks outside of a structure or system. This includes flat folder storage on the Forces servers, 99 communities (Sussex only), as well as information held locally on Force devices.

IAOs are also responsible for data held on legacy systems that are no longer in use but have not been officially decommissioned. They remain accountable for this data until the asset has been officially decommissioned and removed.

8.2 Ownership of unstructured data should be transferred to the new IAO as part of the handover process, when the existing IAO leaves their role.

9. Data Protection Impact Assessments (DPIAs)

9.1 What is a DPIA?

A DPIA is a process to help you identify and minimise the data protection risks of a project. It is a key part of our accountability obligations under the Data Protection Act (2018) and UK GDPR and helps integrate data protection by design and by default into our systems.

9.2 DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material, or non-material.

9.3 The DPIA must:

• describe the nature, scope, context and purposes of the processing;

• assess necessity, proportionality and compliance measures;

• identify and assess risks to individuals; and

• identify any additional measures to mitigate those risks.

9.4 When a DPIA is required:

As part of our obligations under the Data Protection Act (2018) and UK GDPR, we are required to complete a Data Protection Impact Assessment (DPIA) for any project where the processing of personal data will result in a high risk to the data rights of individual data subjects.

9.5 Under Data Protection Act (2018) and UK GDPR, a full DPIA must be completed when a project:

• use systematic and extensive profiling with significant effects;

• process special category or criminal offence data on a large scale; or

• systematically monitor publicly accessible places on a large scale.

9.6 The Information Commissioner's Office (ICO) also requires a full DPIA when a project:

• use innovative technology (in combination with any of the criteria from the European guidelines);

• use profiling or special category data to decide on access to services;

• profile individuals on a large scale;

• process biometric data (in combination with any of the criteria from the European guidelines);

• process genetic data (in combination with any of the criteria from the European guidelines);

• match data or combine datasets from different sources;

• collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);

• track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);

• profile children or target marketing or online services at them; or

• process personal data that could result in a risk of physical harm in the event of a security breach.

9.7 Information Asset Owner responsibilities regarding DPIAs:

It is the responsibility of the IAO to ensure that the screening questions are completed as a minimum, and if deemed necessary by their Force's Information Management Team and the respective Force DPO, a full DPIA is completed for any Information Asset or project that processes or intends to process personal data.

The IAO must ensure that they co-operate fully with their Force's Information Management Team to provide any and all information required in order to complete the DPIA. They may be required to request modifications to the product or process in order for the information risk to be mitigated and the DPIA to be signed off.

The IAO must ensure that the DPIA Screening Questions are completed as early as possible in the procurement / change process and are signed off by their Force's Information Management Team and the respective Force DPO prior to any contract being signed or go-live date.

It is the responsibility of the IAO to ensure that any changes to an asset that impacts the way that personal data is processed through it, shared from it or retained within it, are

reported to their Force's Information Management Team, in order for the DPIA to be updated and re-assessed. The DPIA is a living document and should be reviewed and updated when required to accurately reflect the asset and its use.

As part of the IAO handover process, new IAOs must be made aware of any existing DPIAs for the asset, and their obligations to ensure it is accurate and up-to-date.

Where a decision is not made to carry out a DPIA, the IAO must document the reasons.

10. Contact Information

10.1

Information Management (Surrey)

Information Management (Sussex)

Data Protection Officer (Surrey)

Data Protection Officer (Sussex)

Team: Information Management