The Scottish Ambulance Service

INFORMATION SECURITY POLICY

Version 2.00

DOCUMENT CONTROL SHEET:

Key Information:

Title:	Information Security Policy
Date Published/Issued:	05/04/2022
Date Effective From:	05/04/2022
Version/Issue Number:	V2.00
Document Type:	Policy
Document status:	Approved
Author:	Head of Business Intelligence
Owner:	Senior Information Risk Owner
Approver:	Information Governance Group Policy Review Group Staff Governance Committee
Contact:	Head of Business Intelligence
File Location:	SAS Intranet: Information Governance Policies and Procedures (sharepoint.com)

Revision History:

Version:	Date:	Summary of Changes:	Name:
1.00	13/04/2015	Approved version	KB
2.00	05/04/2022	Approved version	KB

Approvals: This document requires the following signed approvals.

Name:	Date:	Version:
Information Governance Group	03/06/2021	1.05
Policy Review Group	19/11/2021	1.06
Staff Governance Committee	13/12/2021	1.06

Distribution: This document has been distributed to

Name:	Date of Issue:	Version:
Information Governance Group	03/06/2021	1.05
Policy Review Group	19/11/2021	1.06
Staff Governance Committee	13/12/2021	1.06

Linked Documentation:

Document Title:
SAS Information Security Incident Reporting and Management Procedure
SAS Agile Working Policy
SAS Document Security Classification Policy
SAS Business Continuity Management Framework
SAS Data Protection Impact Assessment and Guidance
SAS Risk Management Policy
SAS Data transfer and backup of personal information procedure

SAS ICT Security Policy
SAS Data Protection Policy
SAS Records Management Policy
SAS Social Media Policy
SAS CCTV Policy
SAS Information Governance Policy
SAS Document Storage, Retention and Disposal Policy

Equality and Diversity Impact Assessment:

22 March 2021 – This policy meets the Service's EQIA

1. INTRODUCTION

1.1. Background

The purpose of this Information Security policy is to protect, to a consistently high standard, all information assets.

The benefits of consistent and accurate implementation this policy and associated guidance are:

- Patient, staff and stakeholder confidence that information is handled appropriately
- The ability to share information securely where relevant and where it supports the Service objectives
- Avoidance of breaches and associated reputational damage and financial costs (staff time , fines)
- Compliance with our legal obligations
- Assurance that risks are identified and appropriate controls are implemented and documented

1.2. Aim

The aim of this policy is to preserve:

Confidentiality - Access to Data shall be confined to those with appropriate authority and authority shall be based on a need-to-know basis.

Integrity - Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

Availability - Information shall be available to authorised users and recipients, at the time when it is needed.

1.3. Objectives

The objectives of this policy are to establish and maintain the security of information owned or held by the Service by:

- Providing management direction and support for information security;
- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies including:
    - Agile Working Policy
    - CCTV Policy
    - Data Protection Policy
    - Document Security Classification Policy
    - Document Storage, Retention and Disposal Policy
    - ICT Security Policy
    - Information Governance Policy
    - Information Security Incident Reporting and Management Procedure

  - Records Management Policy
  - Risk Management Policy
  - Social Media Policy

- Identifying any threats to assets, vulnerabilities and impact;
- Ensuring all information is adequately protected to allow the continuation of day-to-day core operations without any loss or reduction to the quality of service.
- Supporting the implementation of new computerised systems and facilities in accordance with Strategic plans;
- Ensuring security is an integral part of working with information.

2. SCOPE

This policy applies to all staff employed by the Service, Contractors, Agency Staff, Volunteers and third party suppliers.

This policy is developed to complement and comply with relevant data protection, records management and freedom of information legislation.

3. ROLES AND RESPONSIBILITIES

The **Scottish Ambulance Service Board** has accountability for ensuring that Service has an Information Security Policy and that adequate controls, assurance and governance are in place.

The **Chief Executive** has ultimate responsibility, on behalf of the Service, for the secure operation of all information systems. This responsibility is delegated to the respective Senior Information Risk Owner (SIRO).

The **Senior Information Risk Owner (SIRO)** is responsible for implementing and leading the Information Governance (IG) risk assessment and management processes within the Service and to advise the Board on the effectiveness of information risk management across the Service.

The **Caldicott Guardian (Medical Director)** is responsible for facilitating the understanding and awareness of individual and Service-wide responsibilities for maintaining the confidentiality of patient identifiable information. It is their responsibility to ensure that all such activities are proportionate and lawful.

The **Data Protection Officer (DPO)** is responsible for providing advice and monitoring compliance with Data Protection Legislation, and is the first point of contact in the Service for data protection matters. The DPO reports to the SIRO and directly to the Board in relation to data protection matters.

The **Information Security officer (ISO)** has the responsibility of providing technical leadership in and guidance for the ICT department to deliver resilient and secure ICT systems, which meet the identified security requirements. The ISO leads on the cyber resilience capabilities of the Service. Also responsible for the continuous monitoring and review of relevant policy, procedures and guidance. These policy and procedures are provided to allow efficient working practices, whilst maintaining compliance with required legislation and regulations, such as Data Protection and Network and Information Systems regulations.

The **Head of Corporate ICT - General Manager** is responsible for the effective running of the ICT department and the responsibilities it holds. Providing confidentiality, integrity and availability to information and systems by ensuring the procurement, deployment, development, maintenance, in-life management and incident management functions of the ICT estate are capable of meeting the Services requirements.

The **Head of Information Governance** is responsible for maintaining appropriate policies and guidance for staff around the use and processing of data the Service's information assets, including the protection of personal data in line with data protection and data security legislation and regulations.

The Service's **Information Asset Owners (IAOs)** are responsible for ensuring that risk assessments are carried out and appropriate security measures are in place to protect the information they are accountable for.

Senior Managers are responsible for ensuring that good security practices within their area of responsibility are implemented and maintained, by:

- ensuring that they bring published security policies, procedures and guidelines to the attention of their staff;
- ensuring that standards and procedures are followed at all times;
- maintaining an appreciation of the risks associated with the loss of confidentiality, integrity or availability of information;
- ensuring that if any gaps are identified in standards and procedures that they log the gap and associated risks, notify these to the IG team and the SIRO and any other relevant staff, and carry out appropriate work to fill the gap.
- ensuring that all staff attend appropriate data protection and security training;
- setting a good example to staff by applying good security principles to their own work; and
- ensuring departments share information only on 'need to know' principles.

All Staff employed by the Service are responsible for:

- Dealing securely with any information they have access to in the course of their duties;
- Ensuring their actions, when using information systems, conform to this policy, supporting standards, policies and procedures that are relevant to their role, to NHS standards and to legal requirements.
- Ensuring no breaches of information security result from their actions.
- Staff working from home must comply with the Service's Agile Working Policy;
- Immediately reporting any risks, near misses or suspected breaches of information security arising from the actions of themselves or others to their line manager/duty manager and the Information Governance Team, in line with the Service Information Security Incident Reporting and Management Procedure;
- Proactively and routinely attending or participating in Information Governance training provided.
- Correctly mark documentation created by them in line with the SAS Document Security Classification Policy.
- Keep appropriate records of their work in the Service and manage those records in keeping with the SAS Records Management Policy.
- Identifying when a Data Protection Impact Assessment is required (see section 4.9) and following the Service guidance.

4. POLICY FRAMEWORK

4.1. INFORMATION ASSET MANAGEMENT AND RISK ASSESSMENT

The SIRO will ensure that all information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessments and associated mitigation plans to the SIRO for review.

IAOs will assess risks to assets confidentiality, integrity and availability. Where they identify an information risk they will analyse and document the Service impact and plausible worst-case scenarios of an adverse event using the Service Risk Management Process, which is detailed in the SAS Risk Management Policy.

Information Asset Owners will carry out information risk assessments when:

- changes are proposed to their assets, or;
- prior to implementation of new services and information systems, or;
- an information security adverse event has occurred related to their asset

4.2. CONTRACTS OF EMPLOYMENT

Staff security requirements will be considered at the recruitment stage and all contracts of employment will contain an appropriate confidentiality clause. The Service will carry out appropriate recruitment checks, vetting and on-going personnel security.

Information security responsibilities of staff will be included within appropriate job descriptions.

4.3. TRAINING AND AWARENESS

Information Governance training is mandatory and all staff are required to complete the on-line e-learning module within the required time-scales. Completion of the e-learning will be monitored on a regular basis to ensure completion across all areas of the Service.

4.4. INFORMATION SECURITY ADVERSE EVENT MANAGEMENT

All Service information security events, near misses, and suspected weaknesses will be investigated in line with the SAS Information Security Incident Reporting and Management Procedure.

4.5. BUSINESS CONTINUITY

Information Asset Owners will carry out a risk assessment for their information and record systems to ensure that suitable disaster recovery and contingency capabilities are implemented. In rare circumstances, the SIRO may approve the operation of an information system without recovery and contingency facilities where the risk assessment justifies this.

Information Asset Owners will carry out or delegate an annual Business Impact Assessment, in line with the Business Continuity Management Framework. These impact assessment allow for business continuity plans to be reviewed and amended as required.

Recovery procedures will be developed for all operational systems and where relevant an appropriate contingency plan must also be prepared to ensure an acceptable level of service and control is maintained following system failure.

All recovery and contingency plans will be kept up to date with system changes. The Service will test these arrangements initially and at intervals thereafter as part of its ongoing Information Security management programme.

4.6. DOCUMENT SECURITY CLASSIFICATION

The Service will implement appropriate document classifications controls. Further details of the classifications can be found in the SAS Document Security Classification Policy.

4.7. SECURITY OF IT SYSTEMS

The security of IT systems, equipment, networks and applications provided by, or on behalf of the Scottish Ambulance Service and its staff will be managed in line with the SAS ICT Security Policy.

4.8. SECURE DATA TRANSFER

Where there is a requirement to transfer personal data out with the Service appropriate controls will be taken in line with the SAS Data Transfer and Backup of Personal Information Procedure.

4.9. DATA PROTECTION IMPACT ASSESSMENTS

The completion of a Data Protection Impact Assessment must be carried out when:

- A new process is to be established that involves processing of personal data (data relating to individuals);
- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data.
- Introducing any new technology that uses or processes personal data in any way

The Data Protection Impact Assessment template and guidance can be found on @SAS.

5. MONITORING

Monitoring compliance with this document will be monitored via the Information Governance Group, together with independent reviews by Internal Audit on a periodic basis.

The Head Information Governance is responsible for the monitoring, revision and updating of this document on a two yearly basis or sooner if the need arises.