Information Security Incident Management Policy

V1.0
December 2021

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

CONTROLLED DOCUMENT
This document is uncontrolled when downloaded or printed

Document Information

Document Title	Information Security Incident Management Policy
Version	V1.0 - APPROVED
Author	Simon Lacey
Intended Audience	Information Security and Governance Professionals
Owner	Director of Finance – Senior Information Risk Owner (SIRO)
Ratified by	Trust Board
Approved by	Trust Executive Team
Approval date	5th October 2021
Issue date	10th December 2021
To be Review By	End of October 2023

Related Documents

Title	**Owner**
Digital Strategy	Director of Digital
Governance and Privacy Policy	Head of Information Security and Governance

Helpful Contacts

Team	How they can help you	Email	Telephone
Information Security and Governance Team	Most aspects of this policy	Mark.Northcott@scas.nhs.uk	01869 365131
Information Security and Governance Team	Most aspects of this policy	ISGTeam@scas.nhs.uk	
IT Service Desk	Reporting incidents or suspected incidents, how to use IT equipment.	ICTServiceDesk@scas.nhs.uk	03001239802

Contents

1. Introduction

This policy defines the principles with which SCAS must manage information security related incidents, ensure that incidents are identified promptly, responded to efficiently and that recovery is effective. Equally important is that we learn from incidents, so that we can enhance our information security arrangements.

Our incident response looks to support the Information and supporting systems that are vital to SCAS and those we serve and to this end we will protect information and systems regarding their:

Confidentiality	Protecting information so that it is not made available or disclosed to unauthorised individuals, entities, or processes.
Integrity	Preventing information and data from being modified in an unauthorised or undetected manner.
Availability	Ensuring information and system are available, when needed.

This policy supports our digital strategy and our operational strategy.

2. Scope of this policy

This policy applies to all aspects of information technology within SCAS.

In addition, the controls defined within this policy also apply to our suppliers, third-party providers and stakeholders that process SCAS data and services, as defined within our contracts and service level agreements.

Each control has a defined control owner, who is responsible for identifying all relevant stakeholders and subject matter experts to support these controls.

3. Training

This policy is supported by specialist training for the roles that support our incident response. Those that fulfil these roles will be aware of these requirements.

If you feel you have not had sufficient training to allow you to discharge your responsibilities securely, you must inform your line manager, who will support you in sourcing training appropriate to your needs.

4. Policy Concessions

If it is not possible to meet the requirements of a policy control, then a formal concession must be sought from Information Security and Governance Team.

Concessions require a formal risk assessment and are time limited and discretionary.

In all cases where a concession is granted, compensatory controls must be identified and monitored for effectiveness.

5. Sanction

Failure to comply with our policies or discharge the responsibilities defined within them may lead to disciplinary action in line with the Trust's Disciplinary & Conduct Policy.

6. Definitions and Abbreviations

We maintain a standard set of definitions and abbreviations for our information governance and security policies. These can be found on our [LINK] intranet.

7. Equality Impact Assessment

This policy will be applied fairly to all employees regardless of race, ethnic or national origin, colour, or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other relevant factor.

By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

Where there are barriers to understanding, e.g., an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resources Department.

Employees exercising their rights and entitlements under the regulations will suffer no detriment as a result.

The EIA can be found [LINK] here.

8. Roles and Responsibilities

We expect all our staff to work to the highest standards of information security and governance, we are all responsible for discharging our responsibilities securely and seeking assistance when we are not sure how to proceed.

Further information can be found [LINK] here, including specialist information security and governance roles and their responsibilities.

9. Policy Feedback

We welcome feedback on this policy, controls contained within it and ways in which we can make this document more impactful. Please send feedback to the Head of Information Security and Governance.

10. Incident Management

Security Objective:
To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Clause 10.1

Policy Control
All information security incident procedures must align with the Trust's incident management plans, critical incident framework and business continuity plans.

The Head of Information Security and Governance must:

- Review arrangements to ensure alignment, engaging with stakeholders and subject matter experts, as required.

Control Owner
Head of Information Security and Governance.

Clause 10.2

Policy Control
The Head of Information Security and Governance must document procedures for reporting and identifying actual and potential information security incidents and weakness.

These procedures must cover:

- Reports from individuals, stakeholders, and subject matter experts.
- Notifications from third parties (including National Cyber Security Centre,
- NHS Digital, law enforcement, suppliers, clients, etc.)
- Alerts generated by automated means, such as software and hardware.

Control Owner
Head of Information Security and Governance.

Clause 10.3

Policy Control

The Head of Information Security and Governance must document procedures to manage identified information security incidents, which include incident response, recovery, and learning.

Documented procedures, produced with relevant stakeholders, must include:

- Roles and responsibilities
- Triage and impact assessments.
- Classification and severity.
- Logging.
- How to maintain integrity of information and legal constraints. ▪ Investigating the cause of the incident.
- Steps to contain and eradicate incidents.
- Contact details for relevant parties – internal and external.
- Communication plans, with key decision points and reference to stakeholders, including the ICO and data subjects (where relevant).
- Media plan to manage any potential media interest, in conjunction with the communications team.
- Restoration to previous known good state.
- Integrity checks to information.
- Restoring information.
- Identification of actions to relevant owners, including information asset owners.
- Definition of how to close an incident.
- Procedures must be reviewed regularly to ensure they are effective.

Control Owner
Head of Information Security and Governance.

Clause 10.4

Policy Control
The Head of Information Security and Governance must ensure that all incidents are reviewed, once the Trust has recovered, so that the root cause is understood, reducing the risk of a re-occurrence, sharing with stakeholders as appropriate.

- Root cause analysis will be performed on all incidents.
- Incident and near miss learning will be considered for all comparable assets.
- All controls will be reviewed considering the identified learning, to ensure they remain effective.
- Corrective actions will be undertaken to minimise risks of similar incidents occurring.
- The Information Security Steering Group will maintain oversight of
- incidents and the identified learning, escalating where necessary.

Control Owner
Head of Information Security and Governance.

Annex A – Document Governance

Version History

Version	Date	Author	Description/Change Summary
V0.1-v0.4	December 2020	Simon Lacey	Drafting of policy, which capturing comments and from stakeholders.
V0.5	December 2020	Simon Lacey	Submitted to Director of Digital for approval.
V0.6	January 2021	Simon Lacey	Submitted for trust-wide consultation.
V0.7	June 2021	Simon Lacey	Minor changes made
V1.0	December 2021	Simon Lacey	Final version prepared for publication

Review History

Version	Date	Reviewer	Role	Comments

Sources and References

The following sources, references and legislation were consulted, as part of the development of this policy. Links correct at time of publication and will be checked at next review

Links correct at time of publication – please report broken links.
[LINK] General Data Protection Regulation (GDPR) – Data Protection Act 2018 (DPA 2018)
[LINK] ISO 27002.

Stakeholder Community

The following stakeholders were consulted during the writing of this policy and their contribution is acknowledged, with thanks.

Stakeholder	**Role**
Director of Finance and SIRO	Accountable
Director of Digital	Responsible
Head of Information Security and Governance	Responsible
Information Governance Manager	Informed

Annex B – Implementation and Monitoring

Implementation plan

	Action	Owner
1.	Perform gap analysis between policy and what is currently in place.	Head of Information Security and Governance
2.	Develop action plan, based on identified gaps.	Head of Information Security and Governance
3.	Writing supporting procedures, engaging relevant stakeholders and subject matter experts, as required.	Head of Information Security and Governance
4.	Review procedures regularly to ensure they effectively support this policy.	Head of Information Security and Governance

Monitoring plan

	Action	Owner
1.	The Information Governance Steering Group is responsible for monitoring the effectiveness of this policy and will formally document its findings.	Head of Information Security and Governance
1.	Include in the internal audit plan	Head of Audit
2.	Compliance checks of policy controls at least annually	Head of Information Security and Governance

Annex C – Incident Management Process

IDENTIFY

We shall maintain procedures for reporting and identifying suspected and actual information security incidents and security weaknesses.
Policy Principle – 10.1.

RESPOND

We shall maintain procedures to manage identified information security incidents, including incident response.
Policy Principle – 10.2.

RECOVER

We shall maintain procedures to manage identified information security incidents, including recovery.
Policy Principle – 10.2.

LEARN

We will review all incidents, once we have recovered, so that we may understand the root cause, reducing the risk of a reoccurrence.
Policy Principle – 10.3.