Information Governance Aspects of Third-Party Supplier 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 Governance Aspects of Third-Party Supplier Management Policy
Version	V1.0 - APPROVED
Author	Simon Lacey
Intended Audience	Information Security and Governance Professionals, Procurement Professionals and Information Asset Owners.
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
Procurement	Support for the procurement process	Viv.hitchens@scas.nhs.uk	07867449533

Contents

Document Information 2

Related Documents 2

Helpful Contacts 2

1. Introduction 4

2. Scope of this policy 4

3. Training 4

4. Policy Concessions 5

5. Sanction 5

6. Definitions and Abbreviations 5

7. Equality Impact Assessment 5

8. Roles and Responsibilities 6

9. Policy Feedback 6

10. Third Party Management 6

Annex A – Document Governance 10

Annex B – Implementation and Monitoring 11

1. Introduction

The increasing reliance of SCAS in the expertise and services of third parties, necessitates the need to understand and manage our information risk, both with our third parties and their downward supply chains.

Third parties include suppliers of hardware, software, specialists' skills, and cloud service providers.

To manage these risks, we must identify and manage our information risk, so that we can embed our information security requirements within our formal contracts and service level agreements.

Information and information systems that are accessed, or supported by our third-party partners, 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.

2. Scope of this policy

This policy applies to all aspects of working with third party suppliers that support SCAS, including their downward supply chain.

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 the information governance and security mandatory training, which ensures that all staff reach a minimum baseline of understanding so that they can comply with the controls set out within this policy.

If you feel you have had insufficient 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. Third Party Management

Security Objective:
The Trusts information assets, in all forms, must remain protected when accessible to third party suppliers and their supply chain.

Clause 10.1

Policy Control
Information Asset Owners must ensure third party security risks that affect their assets (including personal data) are identified, recorded, and managed.

Information Asset Owners must:

- Work with relevant stakeholders within SCAS and the third party to identify security and privacy risks.
- Consider the criticality and sensitivity of the asset, information, and systems.
- Define the scope of impacted assets.
- Understand the third party’s activity and their supply chain.
- Understand the interface been SCAS and the third party.
- Consider privacy law.

Maintain documentation that supports the identification of third-party risks and those within the supply chain.

Control Owner
Information Asset Owner.

Clause 10.2

Policy Control
The Head of Information Security and Governance must document and make readily available the control requirements applicable to third parties and their supply chain.

The Head of Information Security and Governance must:

- Document the controls that third parties must deploy.
- Make the document readily available and mark as unclassified.
- Base this document on ISO27001 and other related, and relevant, best practice.
- This document must be reviewed regularly, to ensure it remains effective and includes latest best practice.

Control Owner
Head of Information Security & Governance.

Clause 10.3

Policy Control
The Head of Procurement must ensure that third parties formally agree to adopt relevant security controls and privacy requirements identified by the Trust.

The Head of Procurement must include the following within contracts:

- The Trust's right to audit.
- Third party's obligation to deliver independent evidence of the effectiveness of their security controls.
- Third party's obligation to advise SCAS of any changes that may impact Trust assets.
- Standard data protection terms, where third parties may handle personal data on behalf of SCAS.

The Head of Procurement must:

- Ensure that the Data Protection Officer, Information Asset Owner and Caldicott Guardian are informed where third parties may transfer personal data outside of the EEA.

Seek assistance from the Head of Information Security and Governance should the third party be unable to satisfy our security requirements, before contracts are signed.

Control Owner
Head of Procurement.

Clause 10.4

Policy Control
Information Asset Owners must monitor and review third party suppliers to ensure that they achieve a satisfactory level of compliance with the Trust's terms throughout the lifespan of the agreement.

Information Asset Owners must:

- Review third party suppliers regularly, in line with the asset's criticality and risk.
- Consider exercising the Trust's right to audit, when prompted by risk, incidents, or changes within the threat landscape.
- Request independent evidence from third parties that their security controls are effective.
- Engage with relevant stakeholders and subject matter experts across SCAS to support the monitoring effort.

Control Owner
Information Asset Owners.

Clause 10.5

Policy Control
The Head of Procurement must proactively manage changes to the provision of products and services so that SCAS assets remain secure, including during change of supplier or termination of contract.

The Head of Procurement must:

- Maintain and implement a procedure that securely manages changes in third party services.
- Prompt a new risk assessment if there is a possibility that SCAS assets may be adversely impacted.
- Engage relevant stakeholders and subject matter experts across SCAS to assess changes.
- Ensure an exit strategy exists that supports SCAS assets at the end of a contract or upon a change of third party.

Control Owner

Head of Procurement.

Annex A – Document Governance

Version History

Version	Date	Author	Description/Change Summary
V0.1-0.3	10/08/21	Simon Lacey	Development process, including comments from subject matter experts.
V0.4	10/08/21	Simon Lacey	Comments included as part of the consultation process.
V1.0	20/12/21	Simon Lacey	Approved version finalised 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] Freedom of Information Act 2000
[LINK] ISO27001

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 Procurement	Responsible
Head of Information Security and Governance	Responsible
Information Governance Manager	Consulted

Annex B – Implementation and Monitoring

Implementation plan

	Action	Owner
1.	Perform a gap analyse of existing contracts and determine which contracts have not defined security requirements, devising an action plan in the process to close identified gaps.	Head of Procurement
2.	Devise the supplier focused information security policy, which defines our expectations of information security with third parties and their supply chain.	Head of Information Security and Governance
3.	Develop a process to effectively manage third party suppliers, so that security focus can be placed on what matters most.	Head of Procurement
4.	Develop an audit programme so that SCAS can be assured that security expectations are being met.	Head of Procurement

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
2.	Include in the internal audit plan	Head of Audit