South Central Ambulance Service
NHS Foundation Trust

TECHNOLOGY POLICY

Version 1.0

December 2021

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

Document Information

CONTROLLED DOCUMENT
This document is uncontrolled when downloaded or printed.

Document Title	Technology Policy
Version	V1.0 - APPROVED
Author	Simon Lacey
Intended Audience	IT professionals, ICT professionals, Information Asset Owners, Information Security and Governance Professionals, Estates, Clinical Communications & Telemetry
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
Review By	December 2023

Related Documents

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

Helpful Contacts

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

Contents

1. Introduction

This policy defines the security expectations required to ensure that our IT infrastructure can successfully protect the information that we hold. This policy aligns with the requirements of the information standard for information security (ISO27001 and ISO27002).

Information and information systems 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 systems are available, when needed.

This policy supports both 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 apply to our suppliers and the third-party providers that process our 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 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 with this policy, however this policy also requires specialist skills and education, which should be identified with your line manager and your job description.

Information Asset Owners and Information Asset Administrators will receive additional training to ensure they can meet their requirements of the policy.

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 in order 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. Media Handling

Security Objective
To prevent the unauthorised disclosure, modification, removal, or destruction of information stored on media.

Clause 10.1

Policy Control
The IT Manager must ensure that all media must be managed consistently, in line with its sensitivity and using formalised, documented procedures.

The documented procedures must:

- Define the lifecycle of the media, from creation to disposal.
- Define when re-usable media must be wiped, as to be unrecoverable.
- Define when audit trails must be maintained.
- Ensure the safe and secure storage of media, in line with the manufacturer's specifications.
- Define the cryptographic techniques used when media contains personal identifiable information.
- Define the lifespan of any media that may degrade.
- Define when multiple copies of valuable data will be used.
- Define the process for gaining access to media drives.
- Be reviewed regularly, to ensure they remain effective

Control Owner
IT Manager.

Clause 10.2

Policy Control
All media must be disposed of securely, considering the sensitivity of the content, using formalised, documented procedures.

All media containing electronic data must:

- Be disposed of securely, via authorised contractors only, who operate under a contract.
- Have an audit trail of disposal, if they contain personal identifiable information, or information known to be of sensitivity to the organisation.
- Be secured onsite ahead of collection by our approved contractor.
- Have a certificate of disposal, received from the contractor, and maintained, in line with the Trust's records management policies.
- Procedures must be reviewed regularly, to ensure they remain effective.

Control Owner
IT Manager

Clause 10.3

Policy Control
Media must be secured during transportation, so that it is protected against unauthorised access, misuse, or corruption.

Media must:

- Only be sent via approved couriers, operating under contract.
- Be appropriately packaged to protect against physical damage and in line with manufacturers recommendations.
- Be supported by a process that ensures safe arrival at its destination that includes, being logged that it is leaving site, identifying its contents, how it was packaged, when it left site and receipt at its destination.

11. Access Control

Security Objectives:

- To limit access to information and information systems, controlling access and ensuring it is appropriate and secure.
- To enable authorised user access, whilst preventing unauthorised access.
- To make users accountable for safeguarding their authentication information.
- To prevent unauthorised access to systems and applications.

Clause 11.1

Control
Information Asset Owners must define and document the management of access control for logical access, which support the value and criticality of systems and business requirements.

Information Asset Owners must:

- Define and implement the security requirements of applications and information.
- Effectively manage access rights.
- Segregate access control roles and responsibilities.
- Maintain an authorisation process for access requests.
- Regularly review access rights.
- Define roles with privileged access.
- Audit processes at least bi-annually, to ensure they meet expected objectives.
- Document the management of user access, reviewing the document regularly to ensure it remains effective.

Control Owner
Information Asset Owners.

Clause 11.2

Control
The IT manager must ensure that access to networks and network services is restricted to authorised users only.

The IT Manager must work with information asset owners to ensure that users are given access to network and network services that they are authorised to use, and that access supports effective business requirements.

The IT Manager must:

- Document which networks and network services can be accessed by which users.
- Maintain an authorisation procedure to determine who is allowed access to which networks and network services.
- Control access to network connections and network services.
- Define how networks and services can be accessed.
- Determine user authentication requirements for accessing network services, which are informed by formal risk assessment.
- Maintain management controls and procedures to protect network connections and network services, ensuring these controls are documented.
- Determine and document which methods are permitted.
- Monitor the use of network services.

Documentation must be reviewed regularly, to ensure that it remains effective.

Control Owner
IT Manager.

Clause 11.3

Control
The IT Manager must implement a formal user registration and deregistration process to enable and disable access rights.

The IT Manager must:

- Ensure that all users are issued with unique user IDs, so that they are held responsible for their actions.
- Not permit the use of shared user ID's.
- Disable, or remove, user accounts of those leaving the organisation within 24hours of leaving and ideally on day of departure, subject to notification by HR.
- Identify, remove, or disable expired user ID's at least quarterly.
- Ensure that redundant user ID's are not reissued to other users.
- Document the management of user access, reviewing regularly to ensure that it remains effective.

Control Owner
IT Manager.

Clause 11.4

Control
The IT Manager must maintain a formal user access provisioning process to assign or revoke access rights to all systems and services.

The IT Manager must maintain a documented provisioning process which:

- Obtains authorisation from the information asset owner.
- Verifies the level of access granted, ensuring that it is consistent with security and business requirements, such as segregation of duties.
- Ensure that access cannot be activated before the authorisation procedures have been successfully completed.
- Maintains a record of access rights to systems and services granted to a user ID.
- Changes user access rights should their role or function within the organisation change, upon notification.
- Removes access rights to those who leave the organisation.
- Suspends access rights for temporary inactive users, such as long-term

sickness, maternity leave, career break, etc.
- Reviews access rights with information asset owners, at least quarterly.

Documentation must be reviewed regularly, to ensure that it remains effective.

Control Owner
IT Manager

Clause 11.5

Control
The IT Manager must restrict and control the allocation and use of privileged access rights, applying a least privilege model.

The IT Manager must maintain and implement a documented privileged access provisioning process which:

- Obtains authorisation from the information asset owner and Head of ISG.
- Ensures that privileged users formally accept their additional responsibilities.
- Identifies and records a record of those with privileged access for each system or process.
- Allocates privileged access on a need to use and event by event basis.
- Does not allocate privileged access until the provisioning process is complete.
- Allocates privileged access rights to a different user ID than the individual's regular business activities.
- Defines the requirements for the expiration of privileged access rights.
- Review privileged users, to ensure their competence remains in line with their duties and capability.
- Ensure that the unauthorised use of privileged user accounts is prevented.
- Ensures that the confidentiality of secret authentication information is preserved when sharing.
- Ensures that privileged user access rights are disabled on the final day of employment (or before if there could be an increased risk) in the event of a user leaving the organisation.
- Ensure privileged accounts are barred from the Internet or any external sources
- Be protected by further measures like multi factor authentication as agreed with the Head of ISG

Documentation must be reviewed regularly, to ensure that it remains effective.

Control Owner
IT Manager.

Clause 11.6

Control
The IT Manager must implement and maintain a formal management process for the allocation of secret authentication information, such as passwords.

The IT Manager must maintain a documented process for passwords which:

- Considers business requirements and criticality and sensitivity of systems.
- Requires users to sign a statement stating that they will keep authentication information confidential, maintaining the signed statement as part of the terms and conditions of employment.
- Includes the minimum strength and complexity of passwords, as defined by the Head of ISG.
- Allocates a temporary password to new users, which the needs to be changed the first time a user logs in.
- Checks the identity of users ahead of replacing or issuing new passwords.
- Ensures that temporary passwords are unique and are sent securely.
- Requires users to acknowledge the receipt of passwords.
- Ensures that vendor default passwords are changed following installation of software or systems.
- Ensure Default accounts are disabled by default or a risk assessment undertaken if they are required to remain.

Processes must be reviewed regularly, to ensure they remain effective.

Control Owner
IT Manager

Clause 11.7

Control
Information asset owners are responsible for ensuring that users access rights are reviewed at least annually.

The information asset owners must review users access rights at least annually and:

- After changes to job roles, including termination of employment.
- Be reviewed when moving or changing roles within the organisation.
- Be reviewed against role based access controls (RBAC), where defined.
- Privileged access rights must be reviewed more regularly, ensuring that unauthorised privileges have not been obtained.
- A log maintained of privileged accounts, for periodic review.

Processes must be reviewed regularly, to ensure that they remain effective.

Control owner
Information asset owner.

Clause 11.8

Control
The IT Manager must implement and maintain a process for managing changes to the access rights of movers and leavers, including those not directly employed, in a timely manner.

The IT Manager must:

- Upon notification, remove the access rights of employees or third party users within 24 hours of the cessation of employment or contract and ideally on the same day as they cease activities for the organisation.
- Upon notification, make changes to access rights, when requested by the information asset owner.
- Document the IT management process for joiners, movers, and leavers, reviewing regularly.

Control Owner
IT Manager

Clause 11.9

Control
Information Security and Governance Manager must effectively inform users in the safe use of their authentication information, such as passwords.

The Information Security and Governance Manager must:

- Educate users so that they understand the importance of not sharing or writing down their passwords and not using the same password on multiple applications and systems.

Control Owner
Information Security and Governance Manager

Clause 11.10

Control
Information Asset Owners must restrict user's access to systems and applications, on a 'need to know' basis.

Information Asset Owners must:

- Restrict access to data, applications, and networks, dependent on a user's requirements and business need – as defined by the information asset owner.
- Restrict user's ability to read, write, delete, and execute, dependent on their role.
- Ensure that restrictions adequately support business need.
- Document the management of user access requirements, reviewing regularly.
- Provide assurance to information asset owners that controls are effective on a regular basis.

Control Owner
Information Asset Owners.

Clause 11.11

Control
Information Asset Owners must control access to systems and applications via secure log-on procedures.

The IT Manager must document and maintain a log on procedure that:

- Minimises the opportunity for unauthorised access to systems.
- Does not display system or application identifiers, unless log on has been successful.
- Displays a notice that system is only for the user of authorised users.
- Validates the log on information only when all data has been input. ▪ Protects against brute force login attempts.
- Maintains a log of both successful and unsuccessful login attempts.
- Raises a security breach in the event of either a failed or successful breach of logon controls.
- Does not display the password, as it is entered.
- Does not transmit passwords in clear text over a network.
- Locks inactive sessions after 5 minutes and terminates connections after 15minutes of inactivity.
- Restrict connection times for high-risk applications.

Procedures must be reviewed regularly to ensure that they remain effective.

Control Owner
Information Asset Owners.

Clause 11.12

Control
Password management systems must be interactive and enforce quality passwords.

The IT Manager must document and implement a password system that:

- Enforces the use of individual user ID and passwords.
- Allow users to select their own passwords, which includes a confirmation procedure to allow for input errors.
- Enforces a choice of high strength passwords, that are a minimum of 12 characters and must include at least 3 special characters.
- Forces users to change their password upon first login.
- Maintains a record of previously used passwords and prevents the reuse of the last 12 passwords.
- Does not display passwords as they are entered.
- Stores passwords separately from application system data.
- Stores and transmits passwords in protected form.
- Locks users out of account after ten failed log in attempts.
- Is multi factor authentication, where systems support.
- Ensure new systems support multi factor authentication

Control Owner
IT Manager.

Clause 11.13

Control
The IT Manager must restrict the use of utility programs that may be able to override system and application controls.

The IT Manager must ensure that the use of utility programs is restricted and ensure the:

- Restrict the use of utility programs to a minimum practical number of users, authorised by The Head of Information Security and Governance.
- Utility programs are segregated from applications.
- Use of utility programs is logged.
- Unnecessary utility programs are removed or disabled.
- Utility programs are not available to all users.

Control Owner
IT Manager

Clause 11.14

Control
IT Manager must restrict access to program source code.

The IT Manager must:

- Keep program source libraries separate from operational systems.
- Prevent individuals from having unrestricted access to program source libraries.
- Maintain a documented procedure to manage program source code and source libraries, including maintenance and copying.
- Ensure that changes to program source libraries, associated items and the issuing of programming source code is only permitted after appropriate authorisation.
- Keep an audit log of all access to program source libraries.
- Secure program listings to prevent unauthorised access.

Procedures must be reviewed regularly, to ensure that they remain effective.

Control Owner
IT Manager.

12. Cryptography

Security Objectives:

- To define a consistent approach to cryptography, so that information is protected in line with its value, to ensure its confidentiality and integrity can be assured.

Clause 12.1

Control
The IT Manager must effectively manage cryptographic solutions across the organisation, to ensure that information is protected appropriately in line with its value, considering legal requirements and business impact.

Cryptography must:

- Identify and assess legal risk across all relevant jurisdictions.
- Effectively protect the confidentiality and integrity of information, allowing us to determine if critical information has been altered.
- Be used to protect personal information.
- Be used to protect information considered critical to the business (such as intellectual property).
- Be used on all removable media and mobile devices that contain personal data.
- Be authorised by the information asset owner.
- Enable the identity of the originator of critical transitions or communications to be proven (non-repudiation).
- Be kept up to date.
- Be effectively supported by relevant subject matter experts and legal advice.

- Be supported by a documentation, which is reviewed regularly for effectiveness.

The IT Manager must work with the Head of Information Security and Governance to must document and define:

- When encryption must be used, outside the requirements above.
- When risk assessments must be used to determine the type, strength and quality of encryption used.
- How information will be recovered in the event of lost, compromised, or damaged keys.
- How encryption will be implemented across the organisation.
- The impact of encrypted information on controls that rely upon content inspection.
- The systems requirements for implementing cryptographic solutions.
- Define responsibilities for cryptographic solutions.
- Organisational approved solutions.

Control Owner
IT Manager.

Clause 12.2

Control
The IT manager must manage cryptography keys securely and consistently throughout their lifecycle.

Cryptographic keys must be protected against:

- Access by unauthorised individuals or applications.
- Accidental or malicious destruction.
- Unauthorised copying.

The IT Manager must document:

- The lifecycle of cryptographic keys.
- Responsibilities of cryptographic key owners.
- Protection of cryptographic keys.
- Mandatory key disclosure.

The IT Manager must maintain documentation which covers:

- The generation of cryptographic keys, using approved key lengths.
- Secure distribution, activation and storage, recovery and replacement and update of cryptographic keys.

- Immediate deactivation of cryptographic keys – e.g. if a key is compromised, key owner resigns, etc.
- Recovery of cryptographic keys that are lost, corrupted or have expired. ▪ Management of keys that have been compromised.
- Backup and archiving of cryptographic keys and the maintenance of key history.
- Allocation of activation and deactivation dates.
- Restriction of access to cryptographic keys to authorised individuals. ▪ Sharing of cryptographic keys.

Documentation must be reviewed regularly, to ensure that it remains effective.

13. Physical and Environmental Security

Security Objectives:

- To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.
- To prevent loss, damage, theft or compromise of assets and interruption to operations.

Clause 13.1

Control
A security perimeter must be defined and used to protect areas that contain business critical or personal information and information processing facilities.

Head of Estates must understand and document the physical perimeter of their assets and supporting infrastructure by:

- Documenting where assets are located.
- Risk assessing their location.
- Identifying and documenting what controls are necessary to appropriately protect these assets.
- Physically securing critical as assets.

Control Owner
Head of Estates.

Clause 13.2

Control
Buildings that house critical facilities or information must be protected against unauthorised access.

Unauthorised access must be protected against by relevant identified controls, including:

- Locks and bolts on vulnerable doors and windows.
- Employment of security guards.
- Installing closed circuit television (CCTV).
- Installing intruder detection systems on accessible external doors and windows, which must be tested regularly.
- Alarms on fire doors.

Control Owner
Head of Estates.

Clause 13.3

Control
Secure areas must be protected by appropriate entry controls to prevent unauthorised access.

To protect secure areas, we must:

- Ensure that visitors are signed in and out, with both date and times.
- Always escort visitors unless unescorted access has been authorised in writing by the Head of Information Security and Governance or IT Manage on each occasion.
- Ensure visitors are aware of security requirements and emergency procedures.
- Authenticate visitors' identities, using photo ID e.g. passport or driving licence.
- Ensure that access to areas where confidential information is stored or processed is restricted to authorised individuals only.
- Maintain a log of access to all secure areas.
- Ensure visitors always wear visitor badges.
- Provide third party support (i.e. cleaners) with restricted access, which should be monitored.
- Review access requirements regularly, revoking individuals' access when no longer needed.
- Must have the Trust Door Security & Audit system installed on all access points.

Control Owner
Head of Estates.

Clause 13.4

Control
Physical protection for offices, rooms and facilities should be designed and applied.

Physical offices must protect against unauthorised access, or disclosure of information, where appropriate, including:

- Manned reception, or keypad/swipe card to restrict access.
- Blinds or tinted windows, to prevent disclosure of information.
- Closed windows when sensitive discussions are taking place.
- Operate a Clear desk policy when desks are vacated.

Control Owner
Head of Estates.

Clause 13.5

Control
Physical protection against natural disasters, malicious attack or accidents must be designed and applied to ensure information and processing facilities are protected.

The IT Manager must:

- Risk assess for natural disasters, malicious attack, or accidents.
- Risk identified as being above tolerance must be mitigated with appropriate controls.
- Risk assessment must be reviewed regularly.

Control Owner
IT Manager.

Clause 13.6

Control
Procedures for working in secure areas must be designed and implemented.

The Head of Clinical Communications & Telemetry must maintain documentation for working within secure areas that include:

- Any restrictions on taking photos, cameras, or other recording equipment into secure areas.
- Prohibition of lone working in secure areas.
- Fire Prevention awareness and actions (in case of discharge)
- Fortify unused secure areas, for example with locks.
- Procedures must be reviewed regularly to ensure they remain effective.

Control Owner
Head of Clinical Communications & Telemetry.

Clause 13.7

Delivery and loading areas must be controlled to minimise the risk of unauthorised entry. Information and information processing facilities must be isolated away from loading areas.

Control

- Risks associated with delivery and loading areas must be understood, documented, and managed.
- Information, data, and processing facilities must not be left unattended in
- the loading and delivery areas.

Control Owner
Information Asset Owners.

Clause 13.8

Control
Equipment and information must be located and protected to reduce the risk from environmental threats and hazards and opportunities for unauthorised access.

The Head of Estates must:

- Site equipment in secure areas, to prevent unauthorised access.
- Ensure other equipment is not kept in the secure area.
- Ensure equipment is protected from water, dust, vibration, and other identified threats.
- Ensure eating and drinking is prohibited around equipment.
- Humidity and temperature must be controlled and monitored in line with equipment specifications.
- Any sensitive paper information must also be similarly protected.

Control Owner
Head of Estates.

Clause 13.9

Control
Equipment must be protected against power failures and disruption to supporting utilises.

The Head of Estates must consider:

- Equipment manufacturers specifications.
- Capacity requirements. (Time to run etc)
- Inspecting and testing utilities.
- Emergency lighting.

Control Owner
Head of Estates.

Clause 13.10

Control
Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference, and damage.

The Head of Clinical Communications & Telemetry must:

- Ensure cables are appropriately protected for the criticality of the equipment they supply.
- Incoming Junction /end points are in secure areas or suitably protected to the same level.

Control Owner
Head of Clinical Communications & Telemetry.

Clause 13.11

Control
The IT manager must ensure that equipment is correctly maintained to ensure its continued availability and integrity.

The IT Manager must:

- Ensure that equipment is maintained in line with the manufacturer's instructions.
- Ensure that maintenance is only performed by authorised personnel or suppliers.
- Maintain records of all actual and suspected faults.
- Maintain records of all services and repairs undertaken.
- Ensure that maintenance and repair is conducted securely.
- Ensure that repairs and maintenance are inspected before returning to service.

Control Owner
IT Manager.

Clause 13.12

Control
IT equipment and software must not be taken offsite without authorisation.

The IT manager must:

- Implement and maintain a procedure for authorising the removal of assets from site.
- Record when hardware assets have left site, why and who by.
- Record when devices have been returned.
- Consider restrictions on software leaving site.

Control Owner
IT Manager.

Clause 13.3

Control
All items of equipment containing storage media must be verified to ensure that all sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

The IT Manager must:

- Implement and maintain a procedure for removing or overwriting equipment, using appropriate technology. This procedure must be defined by the Head of Information Security and Governance.

Control Owner
IT Manager.

14. Operational security

Security Objectives:

- To ensure that information processing systems function correctly and securely.
- To ensure that information and information processes are protected against malware.
- To protect against loss of data.
- To record events and generate evidence.
- To ensure the integrity of operational systems.
- To protect against the exploitation of technical vulnerabilities.
- To minimise the impact of audit activities on operational systems.

Clause 14.1

Control
The IT manager must document operating procedures and make them available to all applicable users.

The IT manager must ensure that documented procedures exist that include:

- How the system starts up, shuts down and is recovered.
- Backup and scheduling requirements.
- Error handling.
- Maintenance.
- Media handling.
- Environment management.
- Escalation routes.
- Management of audit trails and system log information.
- Monitoring procedures.
- These procedures must be developed with relevant stakeholders, including Information Asset Owners and Head of Information Security and Governance.

The documentation must be reviewed regularly to ensure it is up to date and effective.

Control Owner
IT Manager.

Clause 14.2

Control
The Information Asset Owners must ensure that changes to the organisation, business processes and systems do not negatively affect information security on systems that they own.

The IT manager must:

- Identify and record changes.
- Plan and test changes.
- Assess changes for potential impacts.
- Formally review and approve any changes.
- Roll back in the event of failure.
- Verify that information security requirements are met post change.
- Communicate changes to relevant stakeholders, including the IT Manager and Head of Information Security and Governance.
- Maintain audit logs.
- Define the emergency change procedure in the event of failure.
- Review operating procedures to ensure changes are appropriately
- represented in them.

Control Owner
IT Manager.

Clause 14.3

Control

The IT manager must monitor the use of resources and make projections for future capacity to ensure the system performance supports the business effectively.

The IT manager must:

- Understand capacity requirements, considering business criticality.
- Monitor systems for potential capacity issues.
- Plan to manage capacity issues.
- Document capacity management plans for critical systems, reviewing
- regularly.

Control Owner
IT Manager.

Clause 14.4

Control
The IT manager must separate development, test, and production environments.

The IT manager must:

- Define the criteria for transferring code from development to operational status.
- Separate the development, test, and production environments.
- Manage the change process for testing changes in the production environment.
- Define and document who is permitted access to each environment and any requirements for each login, such as a different profile for test and production environments
- Not copying sensitive or personal data into test environments without approval from the information asset owner and data protection subject matter expert (when relevant).
- Document the separation of each environment, reviewing regularly.

Control Owner
IT Manager

Clause 14.5

Control
The IT manager must ensure that information and systems are protected from malware.

The IT manager must:

- Install and configure malware protection software effectively.

- Keep malware protection software up to date.
- Ensure malware protection is effective.
- Communicate news about malware protection to stakeholders.
- Document the malware protection procedures, reviewing regularly.
- Work closely with relevant stakeholders, including Information Asset Owners and Head of Information Security and Governance.

Control Owner
IT Manager.

Clause 14.6

Control
The IT Manager must make backups of information, software, and system images.

The IT Manager must:

- Understand the business requirements for making backups.
- Define the backup process – including validation, labelling, cycles, and storage.
- Maintain restoration processes.
- Define a retention period, that reflects the records management requirements of the organisation.
- Document backup procedures, reviewing regularly.

Control Owner
IT Manager.

Clause 14.7

Control
The IT manager must generate and secure accurate event logs, which are regularly reviewed.

The IT manager must:

- Ensure the integrity and security of event logs, including limiting access to ICT Staff.
- Ensure that enough storage space is available for storage of logs.
- Ensure that logs are kept for a minimum of 6 months.
- Ensure that logs are lawful and stored lawfully.
- Ensure clock synchronisation.
- Check logs for anomalous behaviour.
- Ensure logs are reviewed by identified stakeholders including Information Asset Owners and Head of Information Security and Governance

- Document procedures for logs, reviewing regularly.

Control Owner
IT Manager.

Clause 14.8

Control
The IT Manager must control the installation of software by both users and onto production systems.

The IT Manager must:

- Define the authorisation process for installation.
- Keep an approved list of Software who may have access to each package ▪ Define the roll back process.
- Identify the training requirements for those performing installation on operational systems.
- Understand the requirements for audit logs on all updates.
- Acquire patches, updates, etc. only from reputable sources.
- Define the archive and maintenance requirements for previous versions of software, configuration details, support software and documentation.
- Document installation processes.

In addition, the IT Manager must:

- Control what software users may install themselves.
- Manage the privileges that permit user installation of software.
- Document user installation procedures, reviewing regularly to ensure they remain effective.
- Disable autorun functionality.

Control Owner
IT Manager.

Clause 14.9

Control
The IT Manager must effectively manage technical vulnerabilities to mitigate risks to information and systems in a timely manner.

The IT Manager must:

- Identify known technical vulnerabilities.
- Scan for specific, identified technical vulnerabilities.

- Remediate identified technical vulnerabilities.
- Manage identified technical vulnerabilities, where no patch is yet available
- Test and evaluate patches, when required.
- Authorise the installation of patches.
- Prioritise patch applications, engaging with stakeholders and addressing critical systems first.
- Maintain an emergency patching process, so that information risk is considered when there is a requirement to deploy patches outside of the usual schedule.
- Document a technical vulnerability management procedure, reviewing regularly to ensure effectiveness.
- Work closely with Information Asset Owners and Head of ISG.
- Inform and seek approval from the Head of ISG for any vulnerabilities and remediation.

Control Owner
IT Manager.

Clause 14.10

Control
The Information Asset Owner must ensure that systems and information remain secure during audit.

Information Asset Owners must:

- Authorise audit access to systems and data, working with the information asset owner to ensure the scope of audit is defined, documented and appropriate.
- Agree the criteria for audits when it may impact business processes.
- Monitor the audit activity, with the information asset owner.
- Document an audit procedure, reviewing regularly to ensure effectiveness.

Control Owners
Information Asset Owners.

15. Communications security

Security Objectives:

- To ensure the protection of information transferred across networks and its supporting information processing facilities.

Clause 15.1

Control

The Head of Clinical Communications & Telemetry must protect the information in systems, applications, and networks.

The Head of Clinical Communications and Telemetry must:

- Secure wireless networks.
- Implement logging and monitoring facilities.
- Implement controls consistently, acknowledging the needs of services.
- Authenticate systems connected to the network.
- Apply restrictions on systems connected to the network.
- Check security compliance of devices connected the network and restrict where required
- Segment the network to restrict horizontal travel.

Control Owners
Head of Clinical Communications and Telemetry.

Clause 15.2

Control
The IT manager must:

- Define the security requirements of each network, engaging with subject matter experts and information asset owner, as required.
- Identify what controls are required.
- Define how network services will be monitored and audited, with the Head of ISG.
- Document network security procedures, reviewing regularly to ensure that it remains effective.

Control Owners
IT Manager.

Clause 15.3

The IT Manager must segregate systems, services, and users.

The IT Manager must:

- Define and secure the perimeter of domains.
- Control access between domains and define what access is permissible.
- Secure and segregate networks.
- Implement authentication, encryption and user level access controls used for wireless networks.
- Document network segregation procedures, reviewing regularly.

Control Owner
IT Manager.

Clause 15.4

Control
The Head of Information Security and Governance must maintain policies, procedures, and guidance to protect the transfer of information both internally and externally.

The Head of Information Security and Governance must:

- Maintain a policy framework that effectively guides staff on secure behaviours when transferring information both internally and externally.
- Advise staff when information needs to be encrypted, prior to transfer.
- Maintain an awareness programme to effectively inform staff of expected secure behaviours.
- Review the policy framework and awareness programmes regularly, to ensure they are effective.

Control Owners
Head of Information Security and Governance.

Clause 15.5

Control
The Information Security and Governance Manager must maintain agreements with third parties to ensure that information is handled securely once it has been shared with them.

The Information Security and Governance Manager must maintain information sharing agreements that included:

- Management responsibilities.
- Standards for packaging and transmission.
- Responsibilities and liabilities in the event of an incident, or unwanted event.
- Information classification requirements.
- Conditions and requirements for onward transmission or sharing.
- Acceptable use.
- Legal restrictions.
- A register of information sharing agreements.

The Information Security and Governance Manager must review information sharing arrangements regularly, to ensure they remain effective.

Control Owner

Information Security and Governance Manager.

Clause 15.6

Control
The IT Manager must protect information transmitted by all electronic methods effectively and in line with its sensitivity and criticality.

The IT Manager must:

- Protect electronic information against unauthorised access, modification, and denial of service.
- Deliver information correctly and securely.
- Provide a reliable service, that satisfies business needs.
- Be lawful.
- Document information protection procedures and standards, reviewing regularly.

Control Owner
IT Manager.

16. Systems acquisition, development, and maintenance

Security Objective:
- To ensure that information security is an integral part of information systems across their entire lifecycle, from design to decommissioning.

Clause 16.1

Control
The Information Asset Owner must include information security within the requirements for a new system or changes to an existing system.

The Information Asset Owner must:

- Understand the needs of the business and users.
- Define criticality of the system.
- Review compliance review outputs.
- Consider policies and supporting standards.
- Review regulations and Law.
- Consider threats and threat intelligence.
- Review incidents and events.
- Consider risk assessments and risk treatment plans.
- Understand recognised best practice.
- Seek the views of stakeholders.

- Document the information security requirements and ensure that stakeholders are satisfied, including the Head of ISG.

Control Owner
Information Asset Owner.

Clause 16.2

Control
The IT manager must protect information involved in the application services passing over public networks against fraudulent activity, contract dispute and unauthorised disclosure and modification.

The IT manager must:

- Understand the level of security required for the impacted information assets.
- Define security requirements for networks, with the Head of ISG.
- Identify applicable security features.
- Define monitoring and audit processes.
- Define how users will be authorised.
- Define authentication requirements.
- Define levels of protection required to preserve confidentiality, integrity, and availability of information.
- Prevent loss or duplication of transmissions.
- Define liability and insurance requirements.
- Document network security procedures, reviewing regularly.

Control Owner
IT Manager.

Clause 16.3

Control
The IT Manager must protect information in applications services passing over public networks to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

The IT Manager must:

- Define the use of electronic signatures by each party involved in the transaction.
- Ensure users secret authentication of all parties are valid and verified.
- Ensure transactions remain confidential.
- Retain the privacy of all parties.
- Define the communication path.
- Define the communication protocols used by all parties.

- Secure the storage of transaction details.
- Embed security in an integrated way throughout the end to end certification/signature process.
- Comply with legal and regulatory requirements.
- Document network security procedures, reviewing regularly.

Control Owner
IT Manager.

Clause 16.4

Control
The Head of Information Security and Governance must define the rules for the development of systems and software security.

The Head of Information Security and Governance must define:

- A secure development environment.
- The security of the software development lifecycle.
- Security requirements in the design phase.
- Security checkpoints within project milestones.
- Secure repositories.
- Security in version control.
- Required application security knowledge.
- Developers' capabilities of avoiding, finding and fixing vulnerabilities.
- Processes for ensuring that third party developers comply with our requirements.
- Documentation for development procedures, reviewing regularly.

Control Owner
Head of Information Security and Governance.

Clause 16.5

Control
Changes to systems within the development lifecycle must be controlled using formal change control procedures.

The IT Manager must:

- Document formal change management procedures for all new systems and major changes.
- Define how and who can authorise changes.
- Define the change submission process.
- Define how the integrity of controls will be assured.
- Identify which assets require change.

- Define the user acceptance requirements.
- Define version control.
- Define audit trail maintenance.
- Define stakeholder engagement requirements.
- Define operational documentation.
- Define schedule for change.
- Review documentation regularly.

Control Owner
IT Manager.

Clause 16.6

The IT Manager must review business critical systems for adverse impact when making changes to operational platforms.

Control

The IT Manager must:

- Ensure the integrity of existing security controls avoiding compromise during change.
- Ensure notification of changes is timely, to allow appropriate tests and reviews.
- Ensure that changes are reflected in business continuity plans.
- Engage with stakeholders.
- Document procedures and review regularly.

Control Owner
IT Manager.

Clause 16.7

Control
The Information Asset Owner must authorise all changes to commercial off the shelf software packages.

The Information Asset Owner must:

- Obtain the vendor's view of the changes and if these will be patched in a later release.
- Define the criteria for allowing changes to software packages.
- Identify risks for both making the changes, against those for not making
- them and ensure these risks are signed off and accepted.
- Define the testing criteria for the changes, including impacts on other assets.
- Define the approval process for making changes.

- Document the changes and retain a record of them.

Control Owner
Information Asset Owner.

Clause 16.8

Control
The IT Manager must establish, document, maintain and apply engineering principles that embed security by design in all systems.

The IT Manager must:

- Devise and embed secure engineering principles that ensure all architecture layers are secure by design.
- Consider the principles and their effectiveness, as new technologies emerge.
- Apply principles to outsourced development.
- Document secure principles, reviewing regularly.

Control Owner
IT Manager

Clause 16.9

Control
The IT Manager must protect system development environments.

The IT Manager must:

- Establish secure development environments.
- Segregate between different environments.
- Control access to the environment.
- Monitor the environments for changes.
- Be lawful.
- Store backups securely.
- Control the movement of data.
- Document the security of environments, reviewing regularly.

Control Owner
IT Manager.

Clause 16.10

Control

The IT Manager must supervise and monitor the activity of outsourced system development.

The IT Manager must:

- Document licensing arrangements, code ownership and intellectual property rights arrangements.
- Include secure design, coding, and testing practices within contractual arrangements.
- Share known risks and threats with the outsourced developer.
- Define acceptance testing requirements.
- Define how security will be built in by design and metrics to ensure the effectiveness of the design.
- Ensure privacy of personal data is maintained and assured.
- Define how testing will be conducted, ensuring code is malware free.
- Define what evidence is required to establish that code is protected against known vulnerabilities.
- Define escrow arrangements.
- Establish the contractual right to audit development processes and controls.
- Document the build environment used to create the deliverables.
- Comply with applicable laws and regulations.
- Document procedures for the management of outsourced development, reviewing regularly.

Control Owner
IT Manager.

Clause 16.11

Control
The Information Asset Owner must test security functionality throughout development.

The Information Asset Owner must:

- Work with stakeholders to define how testing and verification methods performed throughout the development process.
- Prepare test schedules, detailing test inputs and expected outputs.
- Define those who are permitted to conduct tests.
- Define the criteria for independent acceptance tests.
- Document testing procedures, reviewing regularly.

Control Owner
Information Asset Owner.

Clause 16.12

Control
The IT Manager must define and implement acceptance testing criteria for all new information systems, upgrades, and new versions.

The IT Manager must:

- Identify the information security requirements that require testing during acceptance testing.
- Be able to evidence adherence to secure system development practices upon audit or to assure stakeholders.
- Test in a realistic and relevant way.
- Ensure tests are reliable.
- Document testing procedures, reviewing regularly.

Control Owner
IT Manager.

Clause 16.13

Control
The Information Asset Owner must control data selected for test, which must not include personal identifiable information or information considered sensitive to the business or clients.

The Information Asset Owner must:

- Identify what data will be used during test, engaging with stakeholders and the owner of the asset.
- Control and restrict access to test data.
- Gain authorisation before using data in test.
- Comply with law and regulations, including GDPR.
- Understand how data will be erased after testing.
- Maintain audit logs and trails.
- Document testing procedures for selecting data, reviewing regularly.

Control Owner
Information Asset Owner.

Annex A – Document Governance

Version History

Version	Date	Author	Description/Change Summary
0.1 to 0.6	10/02/21	Simon Lacey	Alignment with stakeholder comments and best practice.
v0.7 & v0.8	22/05/21	Simon Lacey	Minor changes to support DSPT compliance.
V0.9	10/08/21	Simon Lacey	Minor changes made in response to consultation process.

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 any broken links.

[LINK] Common Law of Confidentiality
[LINK] Codes of practice for handling information in health and social care
[LINK] General Data Protection Regulation (GDPR) Protection Act 2018 (DPA) 2018
[LINK] Human Rights Act 1998
[LINK] Access to Health Records Act 1990
[LINK] Freedom of Information Act 2000
[LINK] The Caldicott Report
[LINK] Public Records Act
[LINK] The Information Commissioner's Office
[LINK] ISO 27001

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
IT Manager	Responsible
Head of Information Security & Governance	Responsible
Information Governance Manager	Responsible
Information Asset Owners	Responsible
Head of Clinical Communications & Telemetry	Responsible

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.	All control owners
2.	Devise an action plan, which is informed by the gap analyse and risk assessment.	All control owners
3.	Develop relevant processes to support this policy.	All control owners
4.	Develop an audit programme so that SCAS can be assured that security expectations are being met.	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
2.	Include in the internal audit plan	Head of Audit