Policy Group: Information
Version no.: 2.0
Date of issue: February 2024
Approved by: Information Governance Group

Information Security Policy

Contents

TARGET AUDIENCE (including temporary staff)	
People who need to know this document in detail	The Chief Information Security Officer (CISO) & Head of IT Operations
People who need to have a broad understanding of this document	IT Security Team, Director of IT
People who need to know that this document exists	All St Andrew's Healthcare employees and trustees All 3rd Party organisations and contractors

1. **Policy Summary / Statement**
   This Policy defines St Andrew's Healthcare's approach towards Information Security through the implementation of a robust Information Security Management System (ISMS).

2. **Links to Procedures**

   Acceptable Use Standard

3. **Scope**

   Individuals, groups or services covered by this policy include:

   All St Andrew's Healthcare (StAH) employees and trustees
   All 3rd Party organisations and contractors
   The services provided by, for or on behalf of the Charity

   The scope of the ISMS includes:

   • All locations, and operational activities where StAH conducts its operations
   • ISO27001 ISMS Certification Scope (Found at Annex A of the ISMS Manual)

4. **Background**

   StAH recognises the importance of information security and the role it has to play in increasing confidence in the Charity amongst our patients, staff, commissioners, regulatorsand suppliers. Information assets are essential in providing effective patient care and governance. The confidentiality, integrity and availability of information assets must be protected. The delivery of healthcare services to our patients must not be undermined by any breach, loss, or unavailability of our information assets; therefore it is essential that a robust information security management system exists to ensure adequate protection against known and emerging threats. Information security is an important part of the StAH's culture and all individuals within the Charity have a responsibility for maintaining the security of our information assets.

   Any unauthorised deviation from this policy and supporting documentation may result in disciplinary action for staff, and sanction for contractors and third-party suppliers.

5. **Key Requirements**

   To ensure compliance with this policy, StAH must implement and ensure:

   - StAH's approach to information security must satisfy the appropriate clauses, requirements, controls and activities defined within StAH's ISO27001 Information Security Management System (ISMS) and mitigates those risks which impact the Confidentiality, Integrity and Availability of StAH's information processing assets.

   - StAH shall establish objectives for the ISMS on an annual basis, taking into consideration the strategy of the organisation and identified information security risks.

These objectives will be set out by the Chief Information Security Officer (CISO), ITS Security & Digital Forensics and signed off by the Information Security Management Forum.

- StAH must maintain ISO27001:2013 certification

- StAH's approach to Information Security must satisfy the appropriate legal, contractual and statutory requirements as identified by the organisation

- StAH shall ensure a commitment to continual improvement exists within the ISMS

- The ISMS will adopt elements of IT, Cyber Security and Information Governances frameworks and standards, in particular CIS Critical Security Controls, Cyber Essentials+, NIST and GDPR.

6. Roles and Responsibilities

Board of Directors:
The Board of Directors, through the Executive, is ultimately accountable for the design and delivery of all policies and procedures, including this Information Security Policy. They provide strategic oversight and direction to ensure the effective implementation of security measures throughout the organisation.

Chief Executive Officer:
The Chief Executive Officer maintains overall responsibility for ensuring safe practices for patients and staff, which are delivered in part by the development and implementation of, and maintenance and monitoring of compliance to, related policies of the Charity. The CEO plays a crucial role in championing a culture of security and overseeing the organisation's commitment to information security.

SIRO (Senior Information Risk Owner)
The SIRO Approve information governance framework and overall accountability for the information risks within the Charity.

Director of IT:
The Director of IT, reporting to the Board of Directors, has played a lead role in crafting and overseeing the technical aspects of this policy, aligning it with the organisation's IT strategy and objectives. The Director of IT provides expertise in technology matters and ensures the policy reflects the dynamic landscape of IT security.

CISO (Chief Information Security Officer):
The CISO has provided expertise in information security management, ensuring that this policy reflects industry best practices and addresses current and emerging threats. The CISO is responsible for maintaining the highest standards of information security across the organisation and aligning security measures with organisational goals.

DPO (Data Protection Officer):
The DPO, responsible for data protection compliance, has contributed to sections related to data protection and privacy, ensuring alignment with relevant regulations and standards. The DPO plays a critical role in safeguarding sensitive data and upholding privacy principles as outlined in this policy.

IT Operations and Applications Leadership:
Leadership in IT Operations and Applications has provided valuable insights into operational and developmental considerations, ensuring the integration of security measures into IT infrastructure and application development lifecycles. They are instrumental in aligning security with operational and developmental goals, enhancing the overall resilience of the organisation.

IT Security Team
The IT Security Team, is responsible for executing day-to-day security operations, including governance, risk and compliance. This includes monitoring and responding to security incidents, conducting risk assessments, and ensuring compliance with the policies outlined in this Information Security Policy.

Third Parties:
Third parties engaged with the organisation are required to comply with the security requirements specified in contracts. Their involvement includes adhering to the security policies and standards outlined in this Information Security Policy, ensuring a unified and secure environment across all entities associated with the organisation.

All Staff:
While individual staff members are not explicitly named as authors, their collective responsibility is acknowledged. All staff members are vital contributors to the success of this policy by adhering to its principles and actively participating in the organisation's security culture. Every member of the organisation plays a role in safeguarding information and upholding the principles outlined in this Information Security Policy.

7. Monitoring and Oversight

The Chief Information Security Officer (CISO), ITS Security & Digital Forensics has overall accountability for ensuring this policy remains up to date, fit for purpose, and will inform SIRO of any breach and outcomes of any reviews.

8. Diversity and Inclusion

St Andrew's Healthcare is committed to Inclusive Healthcare. This means providing patient outcomes and employment opportunities that embrace diversity and promote equality of opportunity, and not tolerating discrimination for any reason

Our goal is to ensure that Inclusive Healthcare is reinforced by our values, and is embeddedin our day-to-day working practices. All of our policies and procedures are analysed in line with these principles to ensure fairness and consistency for all those who use them. If you have any questions on inclusion and diversity please email the inclusion team at DiversityAndInclusion@stah.org

9. Training

St Andrew's Healthcare provides the following:

- Information Governance, Information Security & Cyber Security Training is mandatory for all new starters
- Annual Information Governance, Information Security & Cyber

Security training to be completed via E-Learning course
- Information Security Team available to provide assistance if necessary via email on InformationSecurityDigitalForensics@stah.org

10. **References to Legislation and Best Practice**

This Policy has been written in order to support the St Andrew's Healthcare with compliance to ISO27001 and best practice guidelines.

ISO (2013). *ISO/IEC 27001 Standard – Information Security Management Systems*. [online] ISO. Available at: https://www.iso.org/standard/27001.

11. **Exception Process**

Any deviations from this policy are to be managed via the dispensation process or captured on the Charity's risk register.

To suggest changes to this policy please contact the Information SecurityTeam ITSecurityandForensics@stah.org

12. **Key changes**

Version Number	Date	Revisions from previous issue
V1.0	06/12/2019	Policy transferred on to the new Charity template
V1.1	02/02/2020	Changed Head of Information security to Head of Architecture & Security, ITS Security & Digital Forensics
V1.2	14/10/2021	Changed Head of Architecture & Security to Information Security & Digital Forensics. Amended some spelling mistakes.
V1.3	04/12/2022	Changed IT Security's email address to the new domain and updated job titles
V1.4	04/03/2023	Review no changes
V2.0	15/12/2023	Changed Job Titles, addition of roles and responsibilities. Change to Chief Information Security Officer (CISO). Moved to new template.