Policy Group: Information
Version no.: 1.4
Date of issue: March 2023
Approved by: Chief Information Officer

INFORMATION SECURITY POLICY

1. Policy Summary

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

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)

Management Statement

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, regulators and 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.

Policy 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 Head of IT Operations and Information Security, 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.

2. Links to Standards

Acceptable use standard

3. Monitoring and Oversight

The Head of IT Operations and Information Security, ITS Security & Digital Forensics has overall accountability for ensuring this policy remains up to date and fit for purpose.

4. 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 embedded in 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

5. 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

6. 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 practise guidelines.

7. How to request a Change or exception to this policy

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 Security Team ITSecurityandForensics@stah.org

8. 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