NHS
Business Services Authority

Information Security Policy

Issue sheet

Document reference	ISMSPOL 001
Document location	- Security and Information Governance webpage on MYHUB - ISMS sub-folder under Clause 5.2
Title	NHSBSA Information Security Policy
Author	Information Security Risk and Business Continuity Manager
Owner	NHSBSA CEO and NHSBSA SIRO
Issued to	All NHSBSA staff
Reason issued	For information/action
Last reviewed	June 2021
Review Cycle	Annual
Date of Equality Assessment	No Impact
Date of Fraud Review	No Impact

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Draft	July 2018	Lead Information Security Risk Manager		
Draft	August 2018	Head of Information Governance and Security Operations Manager		Comments and changes suggested from an IG and ICT Security perspective.
Draft	January 2019	Lead Information Security Risk Manager		Changes made to Policy statement section following BISG comments (Nov 2018) and ISMS IA of Clauses 4-10 (Jan 2019)
V1.0	February 2019	Lead Information Security Risk Manager	BISG	Info sec policy statement signed and ISMSPOL 001 communicated to staff
V1.1	December 2019	Information Security Risk and BC Manager		Annual review process started. The following major elements have been updated; - Information Security policy statement - Updated and revised Information Security

				Objectives. - Included new roles, responsibilities and authorities - Inclusion of new Annex 2
V1.2	January 2020	Information Security Risk and BC Manager	Sent to wider security team for review and comment	Incorporated suggested changes and comments.
V1.3	February 2020	Information Security Risk and BC Manager		To be discussed at ISMS Management Review Group on 10/02/20 and BISG on 20/02/20.
V1.4	February 2020	Information Security Risk and BC Manager		Changes made following ISMS Mgt Review Group comments. BISG approval on 20/02/20
V2.0	February 2020	Information Security Risk and BC Manager	BISG	Approved at BISG 20/02/2020 – communicated to all staff.
V2.1	October 2020	Information Security Risk and BC Manager		Doc updated earlier than annual review period to reflect a number of key impacts/changes; • Separation of Info Sec objectives into a standalone document • CIA definitions now aligned with ISO 27000 • Removal of Annex 2 and replaced with a diagram (Still WIP). Sent to internal security functions for peer-review
V2.2	January 2021	Information Security Risk and BC Manager		Sent to BISG for review and approval
V3.0	January 2021	Information Security Risk and BC Manager	BISG	Approved at BISG
V3.1	June 2021	Information Security Risk and BC Manager		Minor changes made to policy content to reflect NHSBSA's ISO 27001 certification to replace 'alignment' wording contained in the policy document.

Information security policy statement

The NHSBSA is an Arm's Length Body (ALB) of the Department of Health and Social Care (DHSC). We are responsible for providing platforms and delivering services which support the priorities of the NHS, Government and local health economies and in so doing we manage around £35 billion of NHS spend annually.

The volumes and sensitivity of data we hold requires the Leadership Team and Board to be accountable and demonstrate leadership and commitment in relation to information security to support our wider strategic goals and to support staff in their Information Security roles and responsibilities.

Our Information Security objectives continue to align and support the achievement of our strategic goals and CARE values. These are reviewed and tracked by the Information Security Management System (ISMS) Management Review Group as part of our quarterly review meetings.

In order to achieve our Information Security objectives, we continue to effectively manage, monitor and maintain our ISMS which is currently certified to ISO 27001 '*Information Security management system requirements'*. We are committed to continually satisfying the requirements set out in ISO 27001 through our security governance structure and by having an effective ISMS documentation framework in place.

To ensure that our ISMS and security controls are implemented, operating effectively and demonstrating continual improvement, we are committed to determining and providing the necessary resources required to minimise our Information Security risks and effectively respond to the evolving landscape of internal and external threats which we face.

Our ISMS has been designed to ensure that reasonable care is taken to prevent inappropriate access, modification, or manipulation of data from taking place. In practice, this is executed through three core information security principles known as Confidentiality, Integrity & Availability (CIA);

- **C**onfidentiality – property that information is not made available or disclosed to unauthorised individuals, entities, or processes
- **I**ntegrity - property of accuracy and completeness
- **A**vailability – property of being accessible and usable on demand by an authorised entity

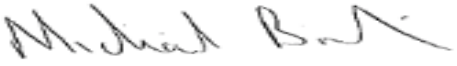
We will achieve these principles by continually monitoring and measuring our ISMS through metrics and Key Performance Indicators (KPIs) to ensure it is operating effectively and achieving its intended outcomes.

We will ensure that we effectively communicate this policy to our staff and contractors and any associated interested parties as appropriate.

Our ISMS will be continually reviewed to ensure its effectiveness is maintained – this will include but is not limited to the following;

- An ISMS Internal Audit Programme to review the effectiveness of the ISMS, security controls and identified corrective actions
- Appropriate metrics and KPIs to continually monitor and measure ISMS performance
- Implementation of key outputs identified from risk treatment and management review activities
- A review of all documentation within the ISMS at appropriately timed intervals

Michael Brodie, Chief Executive NHSBSA



Mark Dibble, SIRO NHSBSA

1. Policy Statement and Authorities

1.1. This policy sets out the organisational intent and importance of Information Security in the NHSBSA with primary aim of preserving the CIA of NHSBSA information assets.

1.2. This policy will serve as a mechanism to achieve our *Information Security Objectives - ISMSOJT 105* which contributes towards the achievement of our strategic goals and CARE values.

1.3. It is the high-level overarching policy for Information Security supported and underpinned by a number of specific information, technical, physical and data protection policies, standards, guidance and procedures which are clearly set out in *ISMSLIS 017 Documentation Asset Log* and available to access here.

1.4. Finally, this overarching policy forms part of our ISMS documented information set as part of our current certification with ISO 27001 '*Information Security management system requirements'*.

2. Audience

2.1 This policy is intended to be read and understood by all NHSBSA staff, contractors, agency staff, Board and ARC members, suppliers, and wider Interested Parties (IPs) where appropriate.

3. Governance, Roles, Responsibilities and Authorities

3.1 There is an established ISMS governance structure in place which is provided at **Annex 1.**

3.2 Individual Terms of Reference (TOR) are in place for each of these key groups.

3.3 The following roles, responsibilities, and authorities in relation to our ISMS are summarised below and overleaf;

Accounting Officer is the Chief Executive and has overall organisational accountability for ensuring that Information Security is operating effectively across the NHSBSA

Staff and contractors must:

- Conform to security policies, standards, procedures and the appropriate protection of information assets
- Be responsible for security and remain accountable for their actions in relation to NHS and other UK Government information and information systems
- Complete mandatory annual training relating to Information Security within the timescales set to ensure that roles and responsibilities are understood
- Safeguard hardware, software and information in their care

The Senior Information Risk Owner (SIRO):

- Be responsible for Information Security and advise the Board on the effectiveness of Information Security across the NHSBSA
- Delegate operational responsibility for Information Security to the Head of Security and Information Governance (HOSIG)
- Provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the ISMS
- Receive training as necessary to ensure they remain effective in their SIRO role

The Head of Security and Information Governance (HOSIG):

- Be responsible for the day-to-day operational effectiveness of this Information Security Policy and its associated policies, standards and procedures
- Lead on the provision of expert advice to the NHSBSA on all matters concerning information security, compliance with policies, setting standards and ensuring best practice
- Provide a central point of contact for information security matters
- Ensure the operational effectiveness of security controls and processes
- Ensure that information security risks are being assessed and treated to an acceptable pre-defined level
- Be accountable to the SIRO for Information Security across the NHSBSA

Information Security Risk and Business Continuity Manager:

- Be responsible for coordinating the ISMS for the NHSBSA
- Be responsible for the implementation and effectiveness of the ISMS and all of its supporting documentation
- Ensure that all information security risks are managed in accordance with *ISMSPCD 014 – Information Security Risk Management Framework*
- Ensure that ISMS Internal Audits are conducted in accordance with *ISMSPCD 008 ISMS Internal Audit Procedure*
- Ensure the delivery of the Security Education, Awareness and Training (EAT) Programme in line with - *ISMSLIS 029 Security EAT Programme*
- Undertake an annual review of all ISMS related documentation and objectives

Information Security Assurance Manager:

- Be responsible for the facilitation of all risk-based information security assurance activities across the NHSBSA
- Lead on information security incident management and ensure all incidents are investigated and mitigated accordingly
- Carry out ISMS Internal Audits and support wider ISMS activity
- Maintain and manage ISMS Policy documentation relating to areas of responsibility

Cyber Security Operations Manager:

- Be responsible for providing Cyber security advice, research, guidance and consultancy, vulnerability, and threat intelligence.
- Provide Cyber security architecture and engineering resource to facilitate safe design and implementation of products and security controls
- Ensure that all technical security risks are managed in accordance with *ISMSPCD 014 – Information Security Risk Management Framework*
- Provision of and monitoring of security systems and controls and alerts thereof
- Investigations of Cyber security incidents

The Head of Technology Operations:

- Lead on the provision of expert advice to the NHSBSA on all matters concerning technical security, compliance with relevant policies, setting standards and ensuring best practice
- Provide a central point of contact for technical security matters
- Ensure the operational effectiveness of technical security controls and processes
- Be accountable to the Chief Technology Officer (CTO) and other bodies for Technical Information Security across the NHSBSA

Information Asset Owners (IAOs) are Heads of Service or equivalent. The IAOs are senior staff members directly accountable to the SIRO and responsible for related services using Information Assets. They are also responsible;

- For understanding what information is held and why
- For knowing what is added and what is removed
- For understanding how information is moved
- For knowing who has access and why
- For ensuring their staff are aware of their Information Security responsibilities
- For ensuring their staff have completed mandatory Information Security training
- For ensuring this policy and its supporting policies, standards and procedures are built into local processes
- Delegate these responsibilities as appropriate to their staff

The Data Protection Officer (DPO):

- Be responsible for advising the NHSBSA on the best course of action to ensure that we always remain compliant with appropriate privacy and data protection legislation as set out in *ISMSLIS 062 - ISMS Compliance Risk Register*

The Caldicott Guardian:

- Be responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data
- Further detailed roles & responsibilities are set out in the *Data Protection and Confidentiality Policy*

4. Compliance

4.1 In applying this policy, the NHSBSA will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

4.2 Compliance with this policy **MUST** be subject to internal and external audit to ensure its effectiveness. The following methods to verify this include but are not limited to;

- Periodic documentation reviews
- Business tool reports
- Reporting within the security governance structure
- Internal and external audits
- Feedback to the policy and standard owner

5. Further Information

5.1 If you require any further information and guidance on the content of this policy, please contact the Security and Information Governance Team for further information.

Annex 1 – ISMS Governance Structure