## Information Security Policy

### Issue sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSARM001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>NHS Business Services Authority Information Security policy</td>
</tr>
<tr>
<td>Author</td>
<td>Head of Security and Information Assurance</td>
</tr>
<tr>
<td>Issued to</td>
<td>All NHSBSA staff</td>
</tr>
<tr>
<td>Reason issued</td>
<td>For information / action</td>
</tr>
<tr>
<td>Last reviewed</td>
<td>December 2017</td>
</tr>
<tr>
<td>Review cycle</td>
<td>Annual</td>
</tr>
<tr>
<td>Date of Equality Assessment</td>
<td>March 2018</td>
</tr>
<tr>
<td>Date of Fraud Review</td>
<td>March 2018</td>
</tr>
</tbody>
</table>

### Revision details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial release</td>
<td>4.09.2007</td>
<td>-</td>
<td>IGSG</td>
<td>In 2.2 add a bullet point as follows “Informing the Chief Executive to assist with the statement of internal control made by him/her”. Replace the paragraph before the first bullet point in 3.3 with “The IGM also carries out the duties below for all corporate directorates bar the Operations directorate, where these daily responsibilities have been delegated to each of five IS Managers, one for each division of the NHSBSA Operations directorate, whose responsibilities include:”. In the second bullet point of 3.4 replace “Information Governance Manager” with</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>V1</td>
<td>09.01.14</td>
<td>G Wanless</td>
<td>ISF</td>
<td></td>
</tr>
<tr>
<td>V2</td>
<td>20.03.14</td>
<td>C Dunn &amp; C Gooday</td>
<td>ISF</td>
<td></td>
</tr>
<tr>
<td>V3</td>
<td>18.02.15</td>
<td>C Gooday</td>
<td>ISF</td>
<td></td>
</tr>
<tr>
<td>V4</td>
<td>03.12.17</td>
<td>ISRS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“Business Manager”
Insert a 3.7 covering Internal Audit

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>09.01.14</td>
<td>G Wanless</td>
<td>ISF</td>
</tr>
<tr>
<td>V2</td>
<td>20.03.14</td>
<td>C Dunn &amp; C Gooday</td>
<td>ISF</td>
</tr>
<tr>
<td>V3</td>
<td>18.02.15</td>
<td>C Gooday</td>
<td>ISF</td>
</tr>
<tr>
<td>V4</td>
<td>03.12.17</td>
<td>ISRS</td>
<td></td>
</tr>
</tbody>
</table>

Changes to Business Unit Area IS Managers

Changes to sections 3, 4 and 5 to reflect PCI DSS compliance.

Annual Review

Revised as part of ISMS work
1 Policy Summary
1.1 This policy forms part of the NHSBSA's initiative to achieve and maintain compliance with ISO 27001 Information Security management system requirements.

2 Introduction
2.1 Information security is fundamental to the operation of all NHS bodies, including the NHS Business Services Authority (NHSBSA), due to the sensitive and confidential patient and personal data captured, along with commercially sensitive information, and the reliance on information systems to process and transmit data to NHSBSA's stakeholders.

2.2 Information security is of paramount importance to the NHSBSA to meet the NHSBSA's primary objectives.

2.3 For the purpose of this policy, information includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on removable and other electronic media or spoken in conversation or over the telephone.

2.4 All information that is created, processed, stored or transmitted (physically or electronically) during the course of NHSBSA business activity is an asset of the NHSBSA and as such is governed by this policy.

2.6 The Information security policy applies to all business functions and covers all information systems, networks, physical environment and relevant people who support those business functions.
2.7 This document:

- sets out the NHSBSA’s policy for the protection of the confidentiality, integrity and availability of its assets, that is hardware, software and information handled by information systems, networks and applications
- establishes responsibilities for information security.

3. Objectives, Key Outcomes, Principles

3.1 The objectives of this policy are to ensure the security of the NHSBSA assets, primarily information assets, that is:

- To ensure availability:

  That is, to ensure that assets are available as and when required hence adhering to the organisation’s business objectives.

- To preserve integrity:

  That is, to protect assets from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation’s assets.

- To preserve confidentiality:

  That is, to protect assets against unauthorised disclosure.

3.2 The key outcome of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the NHSBSA by:

- ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
- describing the principles of security and explaining how they will be implemented in the NHSBSA
- introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities
- creating and maintaining within the NHSBSA a level of awareness of the need for information security as an integral part of the day to day business
- protecting information assets under the control of the NHSBSA
- informing the Chief Executive to assist with the Governance statement made by them.

3.3 This policy applies to all information systems (electronic or manual), networks, applications, locations and people based within the NHSBSA.

4. **Responsibilities for security**

**Overall responsibilities**

4.1 Ultimate responsibility for information security (IS) rests with the NHSBSA Leadership Team, but on a day-to-day basis the Information Governance and Security Group (IGSG) and the Head of Security and Information Assurance (HOS&IA) role within the NHSBSA will be responsible for managing and implementing IS policy and procedures.

**Head of Security and Information Assurance (HOS&IA)**

4.2 **HOS&IA responsibilities include:**

- Acting as a central point of contact on IS within the organisation, for both staff and external organisations.
- Ensuring that the appropriate IS policy for the NHSBSA is produced and kept up to date.
- Advising on the content and implementation of the IS Programme.
- Producing organisational standards, procedures and guidance on IS matters for approval by the IGSG.
- Co-ordinating IS activities particularly those related to shared information systems or IT infrastructures.
- Liaising with external organisations on IS matters, including representing the organisation on cross-community committees.
- Reporting to the IGSG on matters relating to IS.

**HOS&IA’s responsibilities (as delegated)**

4.3 The HOS&IA, assisted by the NHSBSA Information Security and Information Assurance Team also carries out the duties above for all corporate business areas.
Line managers’ responsibilities

4.5 Line managers are directly responsible for:

- Ensuring the security of the organisation's assets (i.e. information, hardware and software) used by staff (permanent, temporary or contractor) and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Ensuring that their staff (permanent, temporary or contractor) are aware of their security responsibilities in accordance with the policies of the NHSBSA.
- Ensuring that their staff (permanent, temporary or contractor) have had suitable IS training.

All staff

4.6 All staff (permanent, temporary or contractor) or agents acting for or on behalf of the NHSBSA have a duty to:

- safeguard hardware, software and information in their care
- prevent the introduction of malicious software on the organisation's IT systems
- report on any suspected or actual breaches in security
- be responsible for the operational security of the information systems they use
- comply with security procedures. Failure to do so may result in disciplinary action.

Internal audit

4.7 The NHSBSA will regularly audit its information security management practices for compliance with this policy.

The audit will:

- identify areas of operation that are covered by the NHSBSA’s policies and identify which procedures and/or guidance should comply to the policy
- annually cover compliance with Payment Card Industry (PCI) Data Security Standard (DSS)
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the management of information security, and use a subsidiary development plan if there are major changes to be made
• set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
• highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the IGSG.

5. Legislation and contractual compliance

5.1 The NHSBSA is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the NHSBSA, who may be held personally accountable for any breaches of security for which they may be held responsible. The NHSBSA will comply with the following legislation and other standards as appropriate:

• General Data Protection Regulation (GDPR)
• Access to Health Records 1990
• Access to Medical Reports Act 1988
• Human Rights Act 1998
• Freedom of Information Act 2000
• Regulation of Investigatory Powers Act 2000
• Crime and Disorder Act 1998
• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
• Obscene Publications Act 1959 and 1964 amendments
• Communications Act 2003
• Protection of Children Act 1978 and 1999 amendments
• Copyright, Design and Patents Act 1988
• Protection from Harassment Act 1997
• Equalities Act 2010
• Computer Misuse Act 1990
• PCI DSS
6. Policy framework

6.1 Information security awareness training

Information security awareness training will be included in the staff induction process. An ongoing awareness programme will be established in order to ensure that staff awareness is refreshed and updated annually.

6.2 Contracts of employment

Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. Security requirements will be included in job definitions.

6.3 Security control of assets

Every asset (hardware, software, application or data) will have a named custodian who will be responsible for the security of that asset.

6.4 Access controls

Only authorised personnel who have a business need will be given access to restricted areas containing information systems.

6.5 User access controls

Access to information will be restricted to authorised users who have a business need to access the information.

6.6 Computer access control

Access to computer facilities will be restricted to authorised users who have a business need to use the facilities.

6.7 Application access control

Access to data, system utilities and program source libraries will be controlled and restricted to authorised users who have a business need to use the applications. Authorisation to use an application will depend on the availability of a licence from the supplier.
6.8 Equipment security

In order to minimise loss of, or damage to, all assets, equipment will be physically protected from security threats and environmental hazards.

6.9 Computer and network procedures

Management of computers and networks will be controlled by standard procedures that have been authorised by the IGSG.

6.10 Security incidents and weaknesses

All security incidents and weaknesses are to be reported. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

6.11 Protection from malicious software

The NHSBSA will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to adhere fully with this policy. Users must not install software on the NHSBSA’s computing assets. Staff breaching this requirement may be subject to disciplinary action.

6.12 Removable media

Removable media containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the NHSBSA’s equipment. Users breaching this requirement may be subject to disciplinary action.

6.13 Monitoring system access and use

An audit trail of system access and use must be maintained and reviewed on a regular basis.

6.14 Accreditation of information systems

The NHSBSA will ensure that all new information systems, applications and networks include a security policy and plan and are approved by the HOS&IA before they commence operation.
New information systems within the scope of PCI DSS must be penetration tested and vulnerability scanned, with issues remediated before going live.

6.15 System change control

Changes to information systems, applications or networks must be reviewed and approved by the HOS&IA.

6.16 Intellectual property rights

The NHSBSA will ensure that all information products are properly licensed and approved by the HOS&IA. Staff must not install software on the NHSBSA’s computing assets. Staff breaching this requirement may be subject to disciplinary action.

6.17 Business continuity and disaster recovery plans

The NHSBSA will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

6.18 Reporting

The HOS&IA will keep the IGSG informed of the information security status of the NHSBSA by means of regular reports.

6.19 Policy audit

This policy will be subject to audit by NHSBSA’s internal auditors.

6.20 Further information

Further information and advice on this policy can be obtained from the HOS&IA.
7. **Validity of this policy**

7.1 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 political affiliation.

In accordance with our Equality Analysis Procedure, an equality analysis has been undertaken on this policy.

7.2 This policy must be reviewed annually under the authority of the NHSBSA Leadership Team members. Associated IS standards should be subject to an ongoing development and review programme.

8. **Related policies, standards and procedures**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Policy</td>
<td>This policy is to ensure that staff are given the relevant support to ensure they are aware of what is acceptable use of any computer system owned or operated by the NHSBSA and therefore can apply procedures accordingly.</td>
</tr>
<tr>
<td>Data Protection and Confidentiality Policy</td>
<td>This policy sets out roles and responsibilities when personal data is being processed to ensure the rights and privacy of individuals are respected, ensuring compliance with current Information Rights legislation.</td>
</tr>
<tr>
<td>Records Management Policy</td>
<td>This policy promotes the effective management and use of information, recognising its value and importance as a resource for delivering NHSBSA objectives.</td>
</tr>
</tbody>
</table>
| Business Continuity / Disaster Recovery Policy       | This policy:  
- ensures that all business Continuity Management (BCM) activities are conducted and implemented in an agreed and controlled manner  
- ensures that the NHSBSA achieve a business continuity capability that meets changing business needs and is appropriate to the size, complexity and nature of the NHSBSA  
- puts in place a clearly defined framework for the ongoing BCM capability |
9. **Penalties**

Any staff that violate this policy may be subject to disciplinary action up to and including dismissal, including criminal prosecution.