Business Services Authority

Security Policy

Acceptable Use Policy

Issue sheet

Document reference	ISMSPOL 083
Document location	- Security and Information Governance webpage on MYHUB - ISMS sub-folder under A.5 Info Sec Policies
Title	NHSBSA Acceptable Use Policy
Author	Information Security Risk and Business Continuity Manager
Owner	Head of Security & Information Governance
Issued to	All NHSBSA staff
Reason issued	For action
Last reviewed	December 2020
Review Cycle	Annual
Date of Equality Assessment	Wellbeing & Inclusion Analysis carried out on the 21/01/19.
Date of Fraud Review	Detailed within policy.

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release 1.0	14.11.2008	-	IGSG	
1.1	26.11.2008		NHSBSA NJC	
1.2	30.3.2010	G Wanless	IGSG	
1.3	26.7.2010	G Wanless	IGSG & NJC	
1.4	20.3.2014	C Dunn & C Gooday		Sections 1, 3, 5, 7 & 9 amendments to reflect PCI DSS Compliance
1.5	11.08.2017	M Sykes		Section 8 amended to include update on social media and other general updates
1.6	11.10.2018	D Howe R Grover		Updated full structure and content.
1.7	November 2018	Lead Information Security Risk Manager		Review of AUP to ensure compliance with ISO 27001 and wider ISMS

1.8	December 2018	Lead Information Security Risk Manager		Further review of AUP to ensure compliance with ISO 27001 & wider ISMS
1.9	March 2019	Lead Information Security Risk Manager		Update to take into account feedback from ISMS Management Review Group members at the 22nd Jan 2019 meeting
1.10	March 2019	Lead Information Security Risk Manager		Update to take into account feedback from Union representatives.
1.11	March 2019	Lead Information Security Risk Manager		Sent to BISG members for review and approval
2.0	April 2019	Information Security Risk and Business Continuity Manager	BISG	Updated Doc approved
2.1	October 2020	Information Security Risk and Business Continuity Manager		Please note this has not been updated due to the business impact of COVID-19. Sent to Security Teams for internal peer-review.
2.2	October 2020	Information Security Risk and Business Continuity Manager		Sent to Unions for review/input.
2.3	November 2020	Information Security Risk and Business Continuity Manager		. Union have provided relevant input. . To be approved at BISG on 30/11/20 . Update hyperlinks at 6.2
3.0	December 2020	Information Security Risk and Business Continuity Manager	BISG	Approved at BISG

1. Policy Statement and Authorities

1.1. This policy defines the NHS Business Services Authority's approach to the Acceptable Use of Assets. This policy gets its authority and approval from **ISMSPOL 001 Information Security Policy** and specifically the following objective/statement of intent;

The NHSBSA shall ensure that the rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

1.2. The purpose of this Acceptable Use Policy (AUP) is to ensure that the applicable and relevant security controls are set in place in line with ISO 27001 – Information Security Management System (ISMS) requirements, the Department for Health & Social Care, the wider NHS, the Security Policy Framework (SPF) and other HMG 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) that use or access the NHSBSA's assets such as information & ICT systems. These will collectively be referred to as 'Users' for the purposes of this policy.

3. Exceptions

3.1 In this document the term **MUST** in upper case is used to indicate an absolute requirement. It is mandatory that all users comply with the requirements detailed in this standard unless a formal exception is raised. Failure to do so may lead to disciplinary action in line with the HR Disciplinary Policy and other associated policies such as the Equality and Diversity Policy.

3.2 Any exceptions to this policy **MUST** be raised initially with the NHSBSA Security & Information Governance team via the **Information Security Policy Exception Management Process (ISMSPOL 023)** and the Information Asset Owner (IAO) must informed. Depending on the severity of the risk assessment, this may be escalated for approval to the Senior Information Risk Owner (SIRO) for formal review and approval.

3.3 Non compliances which are not raised as formal exceptions **MUST** be raised as a security incident – see NHSBSA Security Incident Management Standard Procedure on MYHUB.

3.4 Exceptions to this policy **MUST** be maintained on an appropriate risk register i.e. a team/functional risk register and/or ISMS and Cyber risk registers for accountability, traceability and security governance reporting to senior management.

4. AUP Requirements

Reasonable steps **MUST** be taken by users to ensure that actions and activities undertaken are legal, and not likely to cause harm to the NHSBSA's reputation, our staff or assets. These steps whether that be working remotely or in an NHSBSA office location MUST include the following;

4.1 Not deliberately accessing information or data without authorisation

4.2 Reporting breaches or suspected breaches of any policy, or other security incidents in line with the Security Incident Management Procedure on MYHUB

4.3 Ensure that you familiarise with and understand the NHSBSA Digital and Social Media Policy

4.4 Excessive personal use of the internet and social media during working hours are not permitted

4.5 Ensure that you follow the NHSBSA Phishing process when reporting suspicious emails and attachments

4.6 Keeping up to date with policies, training and guidance provided by the NHSBSA

4.7 In line with the Credential Management Policy ensure that authentication information, such as usernames and passwords, are kept secret and not shared under any circumstances, including to trusted colleagues and ICT staff

4.8 Storing and transporting assets securely and not leaving assets unattended in public areas

4.9 Cardholder data must not be stored or processed by NHSBSA staff nor within the NHSBSA's IT environment. All cardholder data queries must be directed to Capita Pay360 as per the existing process

4.10 Ensure that any mobile phone/laptop/desktop lost or stolen is reported immediately to your local service desk

4.11 You should only use designated and authorised NHSBSA ICT hardware and software unless authorisation has been granted to use personal ICT hardware and software via the Information Security Policy Exception Management Process. Under emergency circumstances i.e. COVID-19 pandemic and other emergency events, this will be dealt with on a case-by-case basis based on the priorities of the NHSBSA at the time.

5. Compliance

5.1 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.

5.2 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

6. Further Information and References

6.1 If you require any further information and guidance on the content of this policy, please contact the NHSBSA Security & Information Governance team for further information.

6.2 Please note the following policy references and where to find them;

- ISMSPOL 001 Information Security Policy
- ISMSPOL 023 Information Security Policy Exception Management Process
- NHSBSA Phishing Process
- HR Disciplinary Process
- Equality and Diversity Policy
- ISMSPCD 035 NHSBSA Information Security Incident Management Standard Procedure
- NHSBSA Digital and Social Media Policy
- Data Classification, Handling and Storage Policy

- ISMSPOL 018 Credential Management Policy