NHS
Business Services Authority

Acceptable use policy

Issue sheet

Document reference	NHSBSAIGM008
Document location	S:\BSA\IGM\Mng IG\Developing Policy and Strategy\Develop or Review Acceptable Use Policy\Current and Final
Title	NHS Business Services Authority Acceptable use policy
Author	[redacted]
Issued to	All staff
Reason issued	For action
Last reviewed	20 March 2014

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Initial release	14.11.2008	-	IGSG	
	26.11.2008		NHSBSA NJC	
	30.3.2010	[redacted]	IGSG	
	26.7.2010	[redacted]	IGSG & NJC	
	20.3.2014	[redacted]		Sections 1, 3, 5, 7 & 9 amendments to reflect PCI DSS Compliance

Contents

Appendices

1. Introduction

1.1 Information plays an essential role in the conduct of the business of the NHS Business Services Authority (NHSBSA).

1.2 The information technology and communications facilities must be used sensibly, professionally, lawfully, consistently with the duties of the role, with respect for colleagues and in accordance with this policy and with the NHSBSA's rules and procedures. The Information Technology infrastructure is either wholly owned by or operated on behalf of the NHSBSA and consequently any information contained therein is owned by the NHSBSA. Due to the nature of the backup processes involved information contained with the infrastructure may be retained for up to a maximum of 10 years.

1.3 All references in this document to NHSBSA shall be deemed to refer to the NHS Business Services Authority, its successor in title, and any other organisation which the NHSBSA wholly or partly controls.

1.4 This policy forms part of the NHSBSA's initiative to achieve and maintain compliance with ISO27001 "Information Security Code of Practice" and Payment Card Industry (PCI) Data Security Standard (DSS).

1.5 This policy will be published on the NHSBSA internet website and any amendments or revisions will be notified to all staff.

2. Objectives, aim and scope

2.1 The objective of this policy is to protect the information assets (e.g. any computer system) owned and used by the NHSBSA, from all threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements, specifically:

- Computer Misuse Act 1990 (CMA)
- Copyright, Design & Patents Act 1998
- Criminal Justice Act 1988
- Data Protection Act 1998 (DPA)
- Freedom of Information Act 2000
- Obscene Publications Act 1959
- Protection from Harassment Act 1997
- Race Relations Act 1976
- Regulations of Investigatory Powers Act 2000
- Sex Discrimination Act 1975
- Telecommunications Act 1984
- The Children Act 1978
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- PCI DSS

It is a criminal offence under the CMA to deliberately attempt to access a system to which no authority has been given.

2.2 The aim of the 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.

2.3 This policy applies to all business areas of the NHSBSA and compliance with its principles is mandatory for computer users accessing any computer system owned and / or operated by the NHSBSA or on its behalf by a third party. Its application extends to the use of all such equipment wherever situated.

3. Responsibilities **Overall**

responsibilities

3.1 Ultimate responsibility for this policy rests with the NHSBSA Leadership Team, but on a day-to-day basis the Information Governance and Security Group (IGSG) and the NHSBSA Head of Internal Governance (HoIG) within the NHSBSA will be responsible

for managing and implementing the policy. The service delivery lead for NHS Help with Health Costs is responsible for PCI DSS compliance.

Contact details for all roles mentioned here are listed in Appendix A.

Head of Internal Governance (HoIG)

3.2 HoIG responsibilities include:

- To develop, maintain and effectively cascade this policy.

Business Unit Information Security Manager (ISM)

3.3 ISM responsibilities include:

- To effectively cascade this policy.

3.4 The Business Unit ISM responsibilities are allocated to the following roles as indicated below:

- NHS Counter Fraud and Security Management
  Head of Information Systems
- NHS Dental Services
  Information Security Manager
- NHS Pensions
  ACI Project Manager and Senior IMT Manager
- NHS Prescription and Patient Services
  Information Services Manager
- NHS Supply Chain Management
  NHSBSA Head of Internal Governance

All employees, third parties, contractors and temporary staff

3.5 Employees, third parties, contractors and temporary staff are responsible for ensuring that they comply with the requirements detailed in this policy.

Any actual or suspected breach of this policy within, or affecting, NHSBSA's systems will be thoroughly investigated, with the assistance of the HoIG or the relevant Divisional Information Security Manager (ISM). Disciplinary action may be taken against NHSBSA employees in line with the relevant disciplinary procedures. Any action taken internally does not preclude prosecution through a Court of Law. In the event of an issue arising from a misinterpretation of this policy, it must be resolved by reference to the HoIG/ISM.

3.4 When the internet is accessed a challenge will be made asking for confirmation of acceptance of this policy before access will be allowed. The text of this challenge is detailed in Appendix B.

Internal audit

3.5 The NHSBSA will annually audit its practices for compliance with this policy.

4. Software copyright compliance

Copyright law, which governs the use of intellectual property, including software, is very straightforward - it is illegal to copy a piece of software unless expressly permitted by the copyright holder.

If caught using illegal copies of software, it is not only the NHSBSA that may face legal proceedings, but individual employees, third parties, contractors and temporary staff may also be charged with criminal and / or civil liabilities. Should such a prosecution be brought, the potential harm to the good name of the NHSBSA is immeasurable.

Legitimate copies of software will be provided to all users who need it, subject to the necessary authorisation having been obtained.

4.1 No employees, third parties, contractors and temporary staff are allowed to make unauthorised copies of any software under any circumstances.

4.2 NHSBSA will not tolerate the use of unauthorised copies of software. Any employees, third parties, contractors and temporary staff illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment, in addition to NHSBSA's disciplinary procedure.

4.3 Only NHSBSA developed software may be given to any non-NHSBSA employees, third parties, contractors and temporary staff, but only if specific authorisation is given.

4.4 Any misuse of software within NHSBSA must be promptly reported using the Information security incident reporting procedure.

4.5 All software to be purchased must be on the approved software list. The HoIG/ISM will ensure that this list is created and maintained accordingly.

4.6 A register of all authorised software will be maintained by HoIG/ISM. All licences and media will be held centrally for all areas of the business apart from NHS Dental Services, NHS Pensions, NHS Prescription Services and Counter Fraud and Security Management Division, where these will be held centrally by each division.

4.7 HoIG/ISM will be responsible for completing the registration of all software with the supplier, installing upgrades and maintaining version control on all software throughout the NHSBSA.

4.8 HoIG/ISM will ensure that all applicable licensing conditions in respect of all software loaded by them are fully met.

4.9 The loading of games, screen savers or unauthorised software on any computer system owned or operated by the NHSBSA is strictly prohibited.

4.10 NHSBSA software must not be loaded on to any computer system not owned or operated by the NHSBSA unless specifically authorised by the HoIG/ISM.

4.11 The use of Freeware and Shareware software is only permitted for appropriate business purposes if the software is shown in the approved software list.

4.12 All NHSBSA computers are regularly audited, as part of the conditions of complying with, but not necessarily being certified to, the standards of the Federation Against Software Theft (FAST).

4.13 All software, information and programmes developed for and / or on behalf of the NHSBSA by employees, third parties, contractors and temporary staff, during the course of their employment remain the property of the NHSBSA. Duplication or sale of such software without the prior consent of the NHSBSA will be an infringement of the NHSBSA's copyright and will be dealt with as a disciplinary matter.

4.14 Software developed for or on behalf of the NHSBSA must comply with this policy.

5. General security

The NHSBSA has procedures in place to deal with the threat of invasive viruses, the risk of theft of hardware and software, the unauthorised access of data and the maintenance of systems security.

5.1 Employees, third parties, contractors and temporary staff must not disclose information relating to NHSBSA's IT facilities to anyone outside of the NHSBSA, without HoIG/ISM's express permission. Any telephone canvassing for information must be passed directly to HoIG/ISM.

5.2 Computers logged onto the network must be locked (press the “windows” key and the letter “L” key at the same time) or logged off the network if left unattended. A password protected screen saver must activate after 10 minutes of inactivity on the PC. If this does not occur, then you should report the matter to your service desk.

5.3 NHSBSA regularly monitors all systems and all unauthorised attempts at accessing systems are investigated.

5.4 Data must be saved on a network drive. The only circumstance where data may be saved to the hard disk or authorised removal media is when a laptop is being taken to a site where the NHSBSA's network is not accessible. In this event, a copy of all the data must be left on the network as a backup.

5.5 Card older data must not be stored outside the NHSBSA's cardholder data environment.

5.6 The responsibility for all data on the network servers lies with HoIG/ISM, who will ensure that regular backups are performed, tracked and stored off site. They are securely destroyed when exceeding the data retention periods.

5.7 Only authorised third parties are permitted to move any NHSBSA IT equipment, whether within an office or to another site, unless specifically approved by HoIG/ISM.

5.8 No peripheral device of any kind (e.g. digital cameras, PDAs, USB pen drives, etc.) may be installed or configured on any NHSBSA computer, unless specifically approved by HoIG/ISM.

5.9 Disposal of NHSBSA IT equipment will be arranged by HoIG/ISM with due regard to legal (software compliance) and environmental issues, ensuring that the appropriate hardware and software registers are updated. Cardholder data will be securely destroyed in compliance with the PCI DSS.

5.10 NHSBSA is governed by the DPA and may only process personal data for specific purposes. Personal data may not be held on any NHSBSA computer without the authorisation of the HoIG as part of that role is to be the NHSBSA Data Protection Officer.

6. Password policy

6.1 All computer users are given a username and password; these are unique and must not be shared with any other employees, third parties, contractors and temporary staff.

6.2 Passwords must not be written down.

6.3 Passwords must be hard to guess and must contain at least eight characters. The minimum password requirement is that it has to include three of the four following types of character:

- Number
- Lower case letter

- Upper case letter
- Special character such as !#£$.

6.4 Passwords must be changed at regular intervals; systems will be configured to automatically force password changes every 28 days and to prevent re-use of the user's previous 12 passwords.

6.5 Password changes will be automatically prompted for when a password expires. To complete a password change the current password will need to re-entered and a new password entered twice. The password will be validated to ensure it matches the guidelines in Appendix C. Any typing mismatches between the new password and the retyped new password will result in the password change process being repeated.

6.6 An account will be locked after three failed password attempts.

6.7 Two factor authentication is required for remote users connecting to the network:

- First-time users will be forced to change their password at first logon
- User's account will be locked after three failed logins until unlocked
- Leavers will have their account access removed within five days by the line manager requesting this from the relevant IT service provider.

6.8 For further password guidelines please refer to Appendix C.

7 Email acceptable usage

The NHSBSA provides email to assist employees, third parties, contractors and temporary staff in the performance of their jobs and its use should be limited to official NHSBSA business.

However, incidental and occasional personal use of email is permitted by NHSBSA, with the understanding that personal messages will be treated in the same way as business messages.

7.1 Personal use of the email system must never impact upon normal traffic flow of business related email. NHSBSA reserves the right to purge identifiable personal email to preserve the integrity of the email system. As a general guide, it would not be reasonable to see more than two or three personal emails a day each of no more than one or two short paragraphs in length.

7.2 No employees, third parties, contractors and temporary staff should knowingly use the NHSBSA's email system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or which may be harmful to the NHSBSA. This includes forwarding any received email containing any prohibited material listed below:

Examples of prohibited materials include, but are not limited to:

- sexually explicit messages, images, cartoons or jokes
- unwelcome propositions, requests for dates, or love letters
- profanity, obscenity or libel
- ethnic, religious, or racial slurs
- or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

7.3 All email messages must be sent or received using NHSBSA's email system, the use of any other email systems including internet email is strictly prohibited, unless specifically approved by HoIG/ISM.

7.3.1 Cardholder data must not be transmitted using messaging technologies. If a messaging technology communication is received containing cardholder data it must be deleted and removed from deleted items folder.

7.4 All emails sent or received will be logged and when considered appropriate by NHSBSA, may be monitored, opened and read by appropriately authorised NHSBSA staff. The only exception to this is any business area that is connected to the Government Secure Intranet (GSI) where all emails will be monitored, opened and read.

7.5 E-mails concerning illegal activities must not be sent or forwarded unless they relate to the legitimate business of NHSBSA. HoIG/ISM must be notified immediately should any such e-mails be received. These emails must not be forwarded to anyone unless required by HoIG/ISM.

7.6 The system may not be used for personal financial gain, other than for selling your own personal possessions on either an NHSBSA intranet site or internet sites such as eBay, but with a non-NHSBSA email address.

7.7 The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Also virus warnings come under the same exclusion; the majority of these are false, to check the truth of these messages consult with HoIG/ISM, but do not under any circumstances forward these messages to anyone inside or outside of the NHSBSA.

7.8 All email messages that are sent externally from the NHSBSA will be passed over networks owned by other people, this is not a secure form of communication. If the content of the message could cause embarrassment or problems for the NHSBSA or cause financial loss, should the contents become known, a more secure method should be used.

7.9 The user logged in at a computer will be considered to be the author of any messages sent from that computer. Remember to log-out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should an e-mail be sent from a PC that is logged in to the network by another person. Email addresses should not be disclosed unnecessarily.

7.10 Disclosing email addresses when filling in surveys or other questionnaires will increase the risk of receiving unwanted junk messages.

7.11 Subscriptions to email lists which are not NHSBSA approved are strictly prohibited. The volumes of messages that can be generated are high and there is no control over the content, which may conflict with the conditions stated above.

7.12 Email should not be used to send large attached files (i.e. 10 Megabytes or larger), unless very urgent. Many email systems including those used by the NHS will not accept large files, which are returned and may result in overloading NHSBSA's own email system. Secure file transfer such as SFTP or removable media, appropriately encrypted, should be used to send large amounts of data, whenever possible.

7.13 Attachments to email messages should not be opened unless they are expected. Extreme caution should be exercised.

7.14 The forwarding of NHSBSA business related information to personal email accounts is strictly prohibited. The NHSBSA provides a number of solutions for accessing the NHSBSA's email system when away from the office.

8. Internet acceptable usage

NHSBSA will provide access to the internet to all authorised employees, third parties, contractors and temporary staff to assist them in the performance of their jobs. Where access is provided, use should be limited to official NHSBSA business. However it is recognised that there may be occasions when employees, third parties, contractors and temporary staff would wish to use the internet for personal reasons; this is permitted during your own time. This personal usage must be kept to an absolute minimum.

8.1 The use and viewing of internet based email is strictly prohibited.

8.2 Messages must not be posted on any internet message board, social networking sites or other similar web based services that could bring NHSBSA into disrepute, or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as that for email.

8.3 As part of routine security measures, all sites visited are centrally logged and monitored.

8.4 The internet must not be used for illegal activities.

8.5 Internet access may not be used for personal financial gain (other than as allowed for under 7.6), nor should a website be hosted on any NHSBSA equipment without express permission.

8.6 The internet must not be used for participation in online games or the use of active web channels that broadcast frequent updates to PCs, such as the BBC News Ticker Tape services, streaming video or audio, for example, radio stations, unless specifically approved by HoIG/ISM.

8.7 Websites that display material of a pornographic nature, or which contains material that may be considered offensive must not be accessed. Examples of prohibited material are given in Section 7.2. It is recognised that accidental viewing of such material may happen from time to time, in this event the HoIG/ISM must be notified immediately.

8.8 Files from the internet, or any images that are displayed must not be downloaded for personal use. If a file is required from the internet the HoIG/ISM should be contacted - there may be any number of issues concerning copyright, viruses and overall functioning of the computer.

8.9 Email addresses must not be unnecessarily entered on a website. Disclosing email addresses when completing surveys or other questionnaires will increase the risk of receiving unwanted junk messages.

8.10 The person logged in at a computer will be considered to be the person browsing the internet. Remember to log out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should the browsing of the Internet take place from a PC that is logged into the network by another person.

8.11 All internet access must be routed through the NHSBSA’s internet proxy server.

8.12 NHSBSA monitors and logs all internet accesses by individuals and reserves the right to access and report on this information.

9. Clear screen and clear desk policy

9.1 At the end of each day, or when desks/offices are unoccupied, any confidential information must be locked away in pedestals, filing cabinets or secure storage where provided.

9.2 All waste paper, which contains any confidential information or data, must be shredded or placed in a locked confidential waste receptacle. Under no circumstances should this type of waste paper be thrown away with normal rubbish.

9.3 All unattended computers logged into the network must be locked (press the “windows” key and the letter “L” key at the same time) or logged out of the network. Locking computers not only prevents someone else from using the PC, but it also prevents someone from reading information which may be confidential.

9.4 Paper media containing cardholder data must never be left unattended and must be locked in a secure storage facility.

10. Mobile computing policy

10.1 A Mobile Computing Device (MCD) (see the Mobile computing policy for a definition of an MCD) must never be left on view in a car, whether the vehicle is occupied or not.

10.2 A MCD must never be left unattended on any form of public transport or in bars / restaurants or any other public place.

10.3 Care must be taken when using MCDs in public places or unprotected areas outside of NHSBSA's premises to avoid the risk of information being overlooked or overheard.

10.4 The encryption utility must be enabled on all MCDs. This will prevent unauthorised access to data, even if the MCD is stolen. HoIG/ISM can give advice regarding the protection of MCDs.

10.5 Anti-virus software must be up to date. Please contact HoIG/ISM if unsure of current status.

10.6 MCDs must be kept secure as they could contain private and confidential information. HoIG/ISM can give advice regarding safe storage of information on MCDs.

11. Validity of this policy

11.1 This policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles. In accordance with the NHSBSA’s Equality & Diversity policy, this policy will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, trade union membership, disability, offending background or any other personal characteristic.

11.2 This policy must be reviewed annually under the authority of the NHSBSA Leadership Team.

Appendix A
Contact details

[redacted]

Business Unit Information Security Managers (ISMs)

- **NHS Counter Fraud and Security Management**
  [redacted]
- **NHS Dental Services**
  [redacted]
- **NHS Pensions and Student Services**
  [redacted]
- **NHS Prescription and Patient Services**
  [redacted]
- **NHS Supply Chain Management**
  [redacted]

Appendix B

Confirmation of understanding

When you connect to the internet the words shown below will be displayed on the personal computer with an acceptance button to be clicked and hence provides confirmation of your understanding and acceptance of this policy. You are not allowed to access the internet unless you accept the statement below:-

"By clicking on the OK button I am confirming that I have seen and read a copy of the NHSBSA Acceptable Use Policy (*a hyperlink to the policy will be included here*). I understand the terms of the Policy and agree to abide by it. I understand that security software may record the use I make of the Internet, which may include logging the addresses of any web sites and noting what file transfers I make. I have no objection to any monitoring of the use I make of any NHSBSA IT equipment. I understand that any violation of this policy could result in disciplinary action, and possibly dismissal or criminal prosecution."

Appendix C

Password guidelines

1. Poor and weak passwords have the following characteristics:
   - The password contains less than eight characters
   - The password is a word found in a dictionary (English or foreign)
   - The password is a common usage word such as:
     - Names of family, pets, friends, co-workers, fantasy characters, etc.
     - Computer terms and names, commands, sites, companies, hardware, software.
     - Birthdays and other personal information such as addresses and phone numbers.
     - Word or number patterns like “aaabbb”, qwerty, zyxwvuts, 123321, etc.
     - Any of the above spelled backwards.
     - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2. Strong passwords have the following characteristics:
   - Contain both upper and lower case characters (e.g., a-z, A-Z)
   - Have digits and punctuation characters as well as letters e.g., 0-9,
   - Are at least eight alphanumeric characters long.
   - Are not words in any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, etc.

3. Passwords must never be written down or stored online.

4. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "*This May Be One Way To Remember*" and the password could be: "*TmB1w2R!*" or "*Tmb1W>r~*" or some other variation.

5. Do not share NHSBSA passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential NHSBSA information.

6. Here is a list of "don'ts":
   - Don't reveal a password to **anyone.**
   - Don't reveal a password in an email message.
   - Don't talk about a password in front of others.

- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on leave.
- Don’t use the "Remember password" feature of applications (e.g., Internet explorer).

If someone demands a password, refer them to this document or have them call the HoIG.

7. If an account or password is suspected to have been compromised, report the incident to HoIG/ISM and change all passwords.

8. Password cracking or guessing may be performed on a periodic or random basis by the HoIG. If a password is guessed or cracked during one of these scans, the user will be required to change it.

9. Any queries regarding passwords or changing of passwords must be referred to HoIG