NHS
Yorkshire and the Humber

Information Security Policy

Ratified by:	Yorkshire and the Humber Strategic Health Authority Board
Date Ratified:	7 December 2010
Status:	Final
Policy Version:	1.0
Title of originator/author:	Confidentiality and IM&T Security Officer (THIS)
Responsible Director:	SHA SIRO
Issue date:	December 2010
Review date:	December 2011
Target audience:	All Staff that are users of SHA Information Systems

Document Revision Record

Version	Description of change	Reason for change	Author	Date

Contents

1. Introduction

1.1 This document defines the Information Security Policy for Yorkshire and the Humber Strategic Health Authority (the SHA).

The Policy:

a. Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of its information assets: - that is hardware, software and information handled by information systems, networks and applications;
b. Establishes the information security responsibilities;
c. Provides reference to documentation relevant to this policy.

2. Objective

2.1 The objective of this policy is to ensure the security of the SHA's information assets. To do this the Health Informatics Service, on behalf of the SHA will:

Ensure Availability - ensure that assets are available for Users;

Preserve Integrity - protect assets from unauthorised or accidental modification;

Preserve Confidentiality - protect assets against unauthorised disclosure.

2.2 Willful or negligent disregard of this policy will be investigated and dealt with under SHA Disciplinary Procedures.

3. Scope of this Policy

3.1 This policy applies to all staff who have access to SHA information systems (including full-time or part-time employees of the SHA, non-executive directors, contracted third party organisations and individuals (including agency staff), students/trainees, staff on placement with the SHA, and staff of partner organisations with approved access).

3.2 This policy applies to all information, media, systems, networks, portable devices, applications and locations.

4. Policy Statement

4.1 The overall Information Security Policy for the SHA is described below:

SHA information systems, applications and networks are available when needed. They can be accessed only by legitimate users and should contain complete and accurate information. The information systems, applications and networks must be able to withstand or recover from threats to their availability, integrity and confidentiality. To ensure this, the SHA will:

a. Protect all hardware, software and information assets under its control. This will be achieved through compliance with Department of Health standards;

b. Provide both effective and cost-effective protection that is commensurate with the risks to its assets;

c. Implement the Information Security Policy in a consistent, timely and cost effective manner;

d. Act in compliance with all relevant legislation including:

-The Data Protection Act 1998
-Copyright, Designs & Patents Act 1988
-Access to Health Records Act 1990
-Computer Misuse Act 1990
-The Human Rights Act 1998
-Electronic Communications Act 2000
-Regulation of Investigatory Powers Act 2000
-Freedom of Information Act 2000
-Health & Social Care Act 2001

5. Risk Assessment and audit

5.1 The Senior Information Risk Owner (SIRO) is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. These risk assessments will cover all information systems, applications and networks that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

5.2.1 Connecting for Health's Information Governance Toolkit requires the SHA to undertake a self-assessment audit based on defined indicators. The SHA Information Governance lead may request further audit.

5.3 Internal Audit has the ability to undertake an audit of compliance with policy on request.

6 Operating Procedures

6.1 Procedures relating to the operation of systems must be appropriately documented. The procedures should be developed on the basis of an analysis of risks.

6.2 User access control and access rights procedural documentation will be developed for each individual system, on the basis of an analysis of risk.

7 Systems Implementation

7.1 Project Managers and others responsible for implementing systems are responsible for ensuring that effective security countermeasures are produced and implemented as part of any new system or project and for ensuring that all relevant system documentation relating to operating procedures and contingency plans are in place as part of the project. Any systems taken to production must follow the original project specification.

8 Accreditation of Information Systems

8.1 All information systems, applications and networks must be approved by the SHA's Senior Management Team, on the recommendation of the IM&T Strategy Group, which in turn will receive recommendations from the Health Informatics Service, before operation is commenced and that approval must be appropriately documented.

8.2 The SHA, through its agreement with the Health Informatics Service, is responsible for ensuring that the information systems do not pose an unacceptable security risk to the organisation.

9 Malicious Software

9.1 The Health Informatics Service must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

10 Unauthorised Software

10.1 Use of any non SHA -approved software[1] on SHA equipment must be approved by the Health Informatics Service before installation. All software used on SHA equipment must have a valid licence agreement - it is the responsibility of the Information Asset Owner or Responsible User of non SHA-approved software to ensure that this is the case.

11 System Change Control

11.1 Ensure that the relevant Project or Information Asset Owner reviews changes to the security of any information system, application or network. In addition, all such changes must be reviewed and approved by the Health Informatics Service. The HIS and Information Asset Owners are responsible for updating all relevant system documentation.

11.2 The Information Asset Owner may require checks on or an assessment of the implementation.

12 External Network Connections

12.1 The Health Informatics Service must ensure that all connections to external networks and systems are documented and approved.

12.2 The Health Informatics Service must approve all connections to external networks and systems before they commence operation.

12.3 Network Security provision is further outlined within the Network Security Policy.

13 Security Monitoring

13.1 Information Asset Owners must ensure that all operational applications, systems and networks are monitored for potential security breaches. Any potential or actual breaches should be logged in accordance with the SHA's incident reporting policy and reported to the IM&T Strategy Group.

[1] Contact the Health Informatics Service Desk for advice on SHA standard software

14 System Configuration Management

14.1 The Health Informatics Service must ensure that there is an effective configuration management system for all information systems, applications and networks.

15 Technical compliance checking

15.1 The Senior Information Risk Owner must ensure that information systems are regularly checked for compliance with security standards.

16 Disaster Recovery Plans

16.1 The Senior Information Risk Owner must ensure that disaster recovery plans are produced for all critical applications, systems and networks.

16.2 The plans must be reviewed and tested on a regular basis.

17 Mobile computing and communications

17.1 Mobile computing is now common place, with users connecting remotely to systems through laptops, mobile phones, PDAs etc. Equipment in transit is at particular risk of being damaged, stolen or lost. Training procedures and written guidance must be put into place for users to cover these threats. Risk assessments should be carried out to identify encryption requirements, e.g. where personally identifiable or other sensitive information is in use.

17.2 The Senior Information Risk Owner, assisted by the HIS Confidentiality and IM&T Security Officer, must ensure that mobile computing equipment recommendations meet Department of Health guidelines as a minimum.

17.3 Information Asset Owners must ensure that audits of mobile working arrangements are carried out to ensure that users are approved, assets can be accounted for, that secure remote access is used, and that any sensitive or confidential information is securely transported and /or stored.

.

17.4 Use of Network File Servers[2] must be promoted and where possible devices should be configured so that data processed on them is synchronised to the network at the end of a session. If data is saved to the local drive and the device is lost so is the data.

17.5 Further information is available from the Confidentiality and IM&T Security Officer (see section 25).

18 Electronic Transfer of Person Identifiable Data

18.1 Any bulk electronic extract and transfers of person identifiable or sensitive data by portable or removable media, file transfer protocol or email, must be encrypted and authorised in advance. Contact the Confidentiality and IM&T Security Officer (see section 25) who will be able to advice on this process.

---

[2] **Network File Server** – computer hardware with large storage capacity which is held in a highly secure area.

18.2 It is a requirement of the SHA that any electronic bulk transfer of person identifiable or sensitive data is encrypted to a standard advised by the Department of Health.

19 Removable Media - including USB, memory stick, pen drives, external hard disk drives, CD Rom, floppy disk - this is not an exhaustive list.

19.1 Staff and contractors are not permitted to introduce or use any removable media for storing or transfer of person identifiable or sensitive information, other than those provided or explicitly approved for use by the SHA.

19.2 Line managers are responsible for the day to day management and overseeing of removable media used within their work areas to ensure this policy is followed.

19.3 Line managers are responsible for the secure storage of all unallocated removable media.

19.4 Staff who have been authorised to use removable media for the purpose of their job role are responsible for the secure use of those removable media as required by this policy.

19.5 Further information is available from the HIS Confidentiality and IM&T Security Officer (see section 25).

20 Secure Disposal or Re-use of Equipment

20.1 All users must ensure that the Health Informatics Service is issued with all redundant computer equipment, including removable media.

21 Reporting Data Security Breaches and Weaknesses

21.1 Data Security Breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the requirements of the SHA's incident reporting procedure and, where necessary, investigated by the Confidentiality and Information Security Officer.

22 Training and Awareness

22.1 The SHA will make security awareness training available as part of their mandatory Information Governance training programme for all staff to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities.

23 Responsibilities

23.1 The Senior Information Risk Owner is responsible for:

Making arrangements for information security through the implementation of an Information Security Policy for the organisation.

Complying with legal requirements and ensuring that operational compliance is further delegated to the Information Asset Owners and the Confidentiality and IM&T Security Officer (the latter function is carried out by the Health Informatics Service on behalf of the SHA).

Ensuring that where appropriate, staff receive information security awareness training.

Engaging and monitoring the service of The Health Informatics Service to ensure delivery of the policy requirements.

23.2 The Health Informatics Service's role as determined through agreement with the SHA is to:

Implement an effective framework for the management of information security in line with the NHS Information Governance Toolkit.

Assist in the formulation of Information Security Policy and related policies and procedures.

Advise on the content and implementation of the relevant action plans.

Produce organisational standards, procedures and guidance on Information Security matters for approval by the IM&T Strategy Group. All such documentation to be included in the Asset register.

Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.

In line with Department of Health directives, ensure all portable storage devices and removable media supported by the SHA are encrypted at hard disk level to the Department of Health's advised standard.

Liaise with external organisations on information security matters, including where required, representing the SHA on cross-community committees.

Review and approve any changes to the security of any information system, application or network and, in conjunction with Information Asset Owners, update all relevant system documentation.

23.3 The Health Informatics Service's Confidentiality and IM&T Security Service will:

Report to the Senior Information Risk Owner on matters relating to information security.

Act as a central point of contact on information security within the organisation, for both staff and external organisations.

Create, maintain, give guidance on and oversee the implementation of, guidance relating to information security.

Represent the organisation on internal and external committees that relate to information security.

Deliver Confidentiality and Information Security training as part of the SHA's mandatory Information Governance training programme.

Maintain the SHA's Information Governance Toolkit assessment

Provide advice and guidance on:
Policy Compliance
Incident Investigation
IT Security Awareness
IT Security Training
Department of Health guidance

Undertake the Data Protection Act notification process.

Assist with enquires in relation to the Data Protection Act.

Advise users of information systems, applications and networks of their responsibilities under the Data Protection Act, including Subject Access.

Advise on potential breaches of the Act and recommended actions.

Encourage, monitor and check compliance with the Data Protection Act.

Liaise with external organisations regarding Data Protection Act matters.

Promote awareness and provide guidance and advice related to the Data Protection Act as it applies within the organisation.

Promote awareness and provide guidance and advice on other legislation and regulations relevant to Information Security and confidentiality as they apply to the organisation.

23.4 Line Manager's Responsibilities

Line Managers are directly responsible for:

Ensuring the security of the organisation's assets, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations;

Ensuring that their staff are aware of their security responsibilities and comply with all SHA policies and procedures;

Ensuring that their staff undertake mandatory Information Governance training.

23.5 Information Management and Technology (IM&T) Strategy Group

responsibilities

Oversee the delivery of the SHA Information Governance agenda to ensure that all information is stored, processed and managed effectively and legally and with due regard to relevant considerations, including Caldicott principles. The IM&T Strategy Group is also responsible for ensuring that all staff are consistently made aware of their obligations in this area.

Ensuring security is considered when applications and systems are under development or enhancement.

23.6 Information Asset Owners

Information Asset Owners, with advice from the Health Informatics Service, are responsible for reviewing changes to the security of any information system, application or network and for updating all relevant system documentation.

Information Asset Owners must ensure that all operational applications, systems and networks are monitored for potential security breaches. Any potential or actual breaches should be logged in accordance with the SHA's incident reporting policy and reported to the IM&T Strategy Group.

Information Asset Owners are responsible for ensuring that audits of any mobile working arrangements are carried out to ensure that users are approved, assets can be accounted for, secure remote access is used, and that any sensitive or confidential information is securely transported and /or stored.

23.7 User Responsibilities

All staff or agents acting for the SHA have a duty to:

Safeguard hardware, software and information in their care;

Ensure that document files are not saved locally on the hard disk (including the desktop) of SHA computers (if the computer were to be stolen the data would be lost). The SHA recognises that there are rare occasions when saving work files locally may be necessary and in these instances a risk assessment should be undertaken, prior to any files being stored on a computer hard disk.

Ensure that person identifiable or other sensitive information is not stored on portable or removable media (laptops, USB, memory stick) unless the device is supported by the SHA **and** the file or drive has been suitably encrypted to the Department of Health's advised standard by the THIS and approved.

Prevent the introduction of malicious software on the organisation's IT systems;

Report on any suspected or actual breaches in security;

Comply with all information security measures approved by the SHA.

Deliberate misuse of information or systems, or negligently disregard of SHA security measures could result in disciplinary action, including dismissal.

24 Network Accounts

24.1 The SHA reserves the right to enable 3rd party access to users' network files and folders in exceptional circumstances i.e. to make arrangements to cover long term sickness leave. Access must be logged. Further information is available from the contact given at section 25

25 Further Information

25.1 Staff who are unsure about best practice in any of these areas, or who may have concerns about existing practice should seek advice from the Confidentiality & IM&T Security Service which is available Monday to Friday from 9AM to 5PM via The Health Informatics Service Desk on 08451272600 or theservicedesk@this.nhs.uk

25.2 If you do not have any questions the SHA presumes that you understand and are aware of the rules and guidelines in the policy and will adhere to them.

26 Associated Policies, Protocols and Procedures

Network Security Policy
Email Policy
Internet Use Policy
Confidentiality Policy Statement and guidance
Data Protection Policy and Confidentiality Compliance
Information Governance Strategy and Policy
Disciplinary Procedure
Voicing Your Concerns Policy