NHS Borders
IT Security Policy

Document Control	
File Name:	IT Security Policy V2-1.doc
Version No:	2.1
Status:	Approved
Author:	Ian Merritt
Version Date:	02 October 2012
Review Date	October 2014

Authorisation Control		
Policy Owner		Chief Executive
Name:	Signature	Date

VERSION HISTORY

Release	Date	Author	Comments
Draft 0.1	24 February 2004	Ian Merritt	1st Draft
Draft 0.2	07 May 2004	Ian Merritt	2nd Draft
Draft 0.3	01 July 2004	Ian Merritt	3rd Draft following review by policy sub-group
Draft 0.4	16 August 2004	Ian Merritt	4th Draft following review by ITSWG
Draft 0.5	11 January 2005	Ian Merritt	5th draft following Consultation Period
Draft 0.6	23 June 2005	Ian Merritt	Minor amendment to clarify disciplinary action as it pertains to Primary Care contractor staff.
Version 2	23 June 2005	Ian Merritt	Released
Version 2.1	24 May 2012	Ian Merritt	Review – Reference documents updated.
Version 2.1	02 October 2012	Ian Merritt	Approved by Information Governance Committee

AUTHORISING CONTROL

Document Control

Document Name:	NHS Borders IT Security Policy
Version No:	2.1
Date Created:	24 February 2004
Date last amended:	24 May 2012
Approved by:	
	Information Governance Committee
Signature:	..... Date.....
Authorised by:	
	Clinical Executive Operational Group
Signature:	..... Date.....

TABLE OF CONTENTS

Introduction

NHS Borders has a responsibility to its stakeholders to ensure its information assets are protected and its information services are used in a responsible manner.

It is therefore prudent to implement an IT Security policy that clearly sets out your responsibilities and is part of NHS Borders' legal and regulatory obligations.

Adherence to the IT Security Policy and any subsidiary policies, standards and guidelines derived from it, is **Mandatory.**

Policy Principles

The NHS Borders Policy principles with regard to IT Security are:

- We reduce the risk of exposure of NHS Borders business and patient information assets to loss, damage or misuse by means of efficient and cost effective risk measurement, risk management and countermeasure implementation. *[See appendix 1 for details]*
- Everyone in NHS Borders, including contractors and external parties, is responsible for the security of NHS Borders' information. It should be noted that it is the responsibility of all managers to ensure that their staff abide by the letter and spirit of the policy. *[See appendix 2 for details]*
- All NHS Borders legal and statutory obligations to protect its Information will be met. *[See appendix 3 for details]*

Policy Authorisation

The policy is authorised by the NHS Borders Chief Executive and the Medical Director.

It is monitored by NHS Borders Information Governance and is available via the Intranet to all employees. Electronic and hard copies can also be obtained from Information Governance.

Definition

IT Security, as discussed in this policy, relates to the protection of all NHS Borders information assets through the use of its IT facilities or services.*[See appendix 1 for details]*

Applicability

This policy applies to all persons who work for any part of NHS Borders or use any part of the IT infrastructure, whether as an employee, a student, a volunteer, a contractor, a consultant, a supplier or a member of the public.

Compliance

There is guidance available to aid understanding of how to comply with this policy. If in doubt seek advice from the Information Security Lead who will help you fulfil your responsibility for the organisation's IT Security.

All IT based projects, including activities leading to changes in the use of NHS Borders' electronically held information assets, must undertake an IT Security risk assessment in order to ensure that the controls delivered by the solution are appropriate to the control requirements of the Organisation. The Information Security Lead will perform the risk assessment in conjunction with the project manager.

There are also a number of subsidiary policies, standards and guides to supplement this policy. These explain in greater detail what is deemed as acceptable use of NHS Borders' Information Services and can be found on the Information Governance website on the NHS Borders Intranet.

These supporting documents include policies on the use of Internet, Email, Home-working, Information Access (including 3rd parties), Authentication and Data Archiving & Retention as well as security standards on physical, infrastructure, software, mobile computing security and a variety of technologies.

Any case of non-compliance with this and any subsidiary policies may lead to disciplinary action or legal proceedings*.*

In the case of NHS employees, disciplinary action means line management being informed and the relevant HR disciplinary process being invoked. In the case of Primary Care contractor staff not directly employed by NHS Borders, the relevant authority will be advised and expected to take the appropriate action. The relevant authority may be the Practice Manager or Senior Partner or may be the Primary and Community Services manager and Medical Director depending on the issue and person involved. If the seriousness of the incident warrants it, failure to take suitable remedial action may result in the person or Practice being disconnected from the NHS Borders network in order to protect the wider network and N3.

Examples of non-compliance when carrying out your NHS Borders duties or using the organisation's facilities include:

- Copying, loading, buying or using unauthorised/unapproved software.
- Installing or using unauthorised or unapproved hardware. This includes modems, PC/laptops and palmtop equipment, electronic organisers (PDAs), mobile phones, digital cameras and USB memory sticks. The term "unauthorised or unapproved" means any device that is not owned and managed by NHS Borders.
- Accessing, loading or distributing non-work related material such as games, music, video, images, or pornography. The material referred to in this example is not restricted to that considered to be offensive or inappropriate but includes all non-work related material.
- Perpetuating chain mail by forwarding it on to other recipients. A chain mail is an email that encourages the recipient to forward to others. It may promise good fortune or even warn of viruses (but these are normally hoaxes).
- Knowingly introducing viruses or malicious software onto NHS Borders' network. Removing or disabling the anti-virus software will also be covered by this example.
- Gaining un-authorised access to computer systems or their content. This includes accessing patient records (even your own or a family member's) that you do not have a justifiable business reason to do so.

- Improper use of password and access controls. E.g. disclosing your password or using somebody else's.
- Breaching confidentiality by passing on or not actively securing sensitive or confidential information. This includes copying data to unauthorised USB memory sticks that are not supplied by NHS Borders IM&T. See the NHS Borders Information Governance Code of Conduct.
- Utilising NHS Borders IT facilities for unauthorised purposes, including personal use during paid working time. Note: certain types of use are not permitted at any time, e.g. running a personal business or conducting business on behalf of another organisation (e.g. typing and/or distributing minutes for Girl Guides, town committees, charitable organisations, etc.).
- Using personally owned computers to process any NHS Borders information. This example includes taking/emailing NHS Borders documents home to work on.

The list above shows examples only: it must not be considered to be exhaustive.

Monitoring

NHS Borders Information Governance will monitor for breaches in security by the use of Security tools and audits. Breaches in security will be recorded as security incidents and reported to line management and/or HR where applicable. It is also the responsibility of everyone in NHS Borders to report any suspected breaches of this policy.

Education & Awareness

An Information Governance site is available on the NHS Borders Intranet to communicate the policy to you and your responsibilities in complying with it. Where the Intranet is not available and for immediate detailed clarification and guidance on this policy, you should refer to the Information Security Lead.

IT Security awareness presentations are given to all new staff and regular sessions for existing staff can be organised.

Reviews

An annual review of this policy will be undertaken to ensure that the levels of protection in place are commensurate with the value and importance of NHS Borders' assets.

Appendix 1 - IT Security Aims

Risk

We aim to manage the risks to our information that include, but are not limited to, privacy violation, error, fraud, embezzlement, sabotage, terrorism, extortion, service interruption and natural disaster.

Key Protection Areas

We aim to protect our Information Assets by focusing on three key areas:

1 CONFIDENTIALITY

Protecting information from unauthorised access.

2 INTEGRITY

Safeguarding the accuracy and completeness of electronically held information and computer software.

3 AVAILABILITY

Ensuring that information and vital IT services are available to authorised users when required.

Our Information Assets

For the purpose of this policy, the term 'Information Assets' includes:

a) **Information assets:** Patient information, employee information, databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;

b) **Software assets**: all software and associated systems;

c) **Physical assets:** computer and data communications equipment, electronic storage media (tapes, disks, USB flash drives, etc.), other supporting technical equipment (computer power supplies, office cabling, air-conditioning units in computer network rooms), LAN/Server rooms;

As an Organisation, we are committed to maintaining effective IT Security controls to safeguard our sensitive and valuable information assets.

Appendix 2 - Your Responsibilities in detail

Highlighted below are your responsibilities under the policy. If in doubt seek advice. The Information Security Lead will help you fulfil YOUR responsibility for the organisation's IT Security.

Information Users

A user is anyone authorised to use information assets and services and is responsible for:

- The permitted use of PCs and Laptops to access approved services and information.
- Effective and proper use of password and access controls;
- Bringing security exposures, problems and incidents to the attention of management;
- Compliance with NHS Borders' IT Security policies, standards and directives.

Acceptable Use, Password Management and Reporting of Incidents is further explained on the Information Governance Intranet site or, where not available, by contacting the Information Security Lead

Line Managers

IT Security is one of line management's responsibilities. In this context a Line Manager is the manager who authorises a person to become an Information User. Line Managers are responsible, within their functions, for:

- Understanding the assets and services for which they are responsible and the applicable access control requirements;
- Authorising employees to use PCs and/or laptops and ensuring that this equipment is used for approved purposes only;
- The education and awareness of their employees to use information assets and services;
- Reporting all IT Security Incidents to the IM&T Service Desk.
- Ensuring their staff, whether directly or indirectly employed (i.e. contracted), have ready access to and comply with the IT Security Policy and other IT policies.
- Being accountable for implementation of the policy and monitoring for compliance within their management area.
- Control of inventories related to NHS Borders owned mobile and offsite computing equipment (Laptops, PDAs, home-based Desktop PCs, etc.).
- Reporting joiners, movers and leavers for allocation/re-allocation of assets to HR and the IM&T Service Desk.

NHS Point of Contact

For the purposes of this policy and all subsidiary policies, an NHS Point of Contact is the member of staff responsible for engaging members of the public onto NHS Borders projects. In this context therefore, the NHS Point of Contact will assume similar responsibilities toward the member of the public as a Line Manager. The NHS Point of Contact will be responsible for:

- Understanding the assets and services for which they are responsible and the applicable access control requirements;
- Authorising members of the public to use PCs and/or laptops and ensuring that this equipment is used for approved purposes only;
- The education and awareness of the members of the public to use information assets and services;
- Reporting all IT Security incidents to the IM&T Service Desk.
- Ensuring the members of the public have ready access to and comply with the IT Security Policy and other IT policies.
- Being accountable for implementation of the policy and monitoring for compliance within their management area.
- Requesting network accounts for the members of the public and notifying the IM&T Service Desk when the member(s) of the public cease their involvement, in order for any network accounts to be disabled.
- The recovery of any assets loaned or assigned to the member of the public.

Information System Owners

An owner is the manager within a business function who is responsible for a particular NHS Borders System or Application for which they have accepted ownership. Ownership, from a security perspective, conveys authority and responsibility for:

- Classifying applications at the appropriate level of security;
- Ensuring that IT Security access controls are in place;
- Ensuring that a maintained Secure Operating Procedure (SOP) is in place;
- Authorising access to their Application;
- Ensuring Contractors, Suppliers, and Support organisations comply, wherever possible, with this policy and the overarching NHS Statement of Compliance. Where the Contractor, Supplier, or Support organisation cannot comply, it is the responsibility of the Information System Owner to ensure that IM&T is made aware and had a chance to comment, before any system access is granted or business relationship entered into.
- Monitoring the compliant use of their Application;

The owner's responsibility to monitor may be delegated. If IM&T are involved then the owner may also delegate responsibility of ensuring compliance.

Information Service Providers

In this context a Service Provider is a supplier or custodian of information processing services in support of NHS Borders' business operations. This will generally applies to IM&T, who administer and maintain the majority of the IT services that support NHS Borders' electronic information assets but may also refer to external organisations who provide the same function.

Service Providers are responsible for:

- Administering owner-specified business and asset protection controls for information assets in their custody.
- Administration of access to classified information where required;

Custodian responsibility includes the obligation to:

- Exercise sound business judgment;
- Comply with applicable directives and agreements;
- Administer owner-specified business and IT Security controls.

Service Providers may accept delegation of authority to grant access to classified information, but may not reclassify information.

As custodian, the supplier of services must administer access to classified information and provide physical and procedural safeguards. This means that it is the responsibility of the Service Provider to ensure that the Information System Owner's data is held securely and is available to authorised users when required.

Appendix 3 - Statutory Commitments and Codes of Practice

It is the policy of NHS Borders that we should comply with the laws and regulations of the country in which we operate or under which we have any contractual association. In respect of IT Security we need to comply with the following legislations:

Copyright, Design and Patents Act 1988

"An Act to restate the law of copyright, to make provision with respect to devices designed to circumvent copy-protection of works in electronic form; to make the fraudulent application or use of a trade mark an offence."

This act is primarily applied to our use of software and how we must ensure adequate measures are in place to prevent illegal copying or use of such licensed software by any of our employees.

Computer Misuse Act 1990

"An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes"

This act applies to how we use the computers and that employees only use the computers for approved purposes.

Data Protection Act 1998

"*An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information."*

This act makes it incumbent on NHS Borders to ensure certain personal data on individuals is only held and used for the purpose for which it was obtained and that it is processed fairly and legitimately.

Human Rights Act 1998

"An act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes."

The particular part of this act that applies is the right to respect for private life, home and correspondence.

Regulation of Investigatory Powers (Scotland) Act 2000

"An act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications …"

This act places a responsibility on NHS Borders to ensure that any monitoring we conduct on behalf of law enforcement agencies is legitimate.

Public Interest Disclosure Act 1998

"An act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation; and for connected purposes."

This act protects the interests of individuals who, having discovered unsafe, illegal or unauthorised activities being performed, report them to the relevant authorities.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This regulation permits an Organisation to intercept and monitor electronic communications conducted from its infrastructure, whilst maintaining each individual's right to confidentiality.

N3 Statement of Compliance

This is an NHS specific requirement that any third party service provider (apart from General Practices) that wish to access NHS Borders systems remotely, i.e. not from an NHS Borders location, sign up to the N3 Statement of Compliance.

This means any organisation that provides support or other services through N3 must obtain approval from Connecting for Health before they are permitted to connect to NHS Borders IT infrastructure. This access cannot be granted at local level. The external organisation must follow the process documented on http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc.

Codes of Practice

In addition to the legislative requirements above, NHS Borders is committed to complying with recognised best practice in Information Security as documented in the ISO/IEC 27000 series of international standards.

ISO/IEC 27002:2005 ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organisational activities.

ISO 27799:2008 ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard.

ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

ISO 27799:2008 applies to health information in all its aspects; whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.

Appendix 4 – Health Service Guidance Documents.

In addition to the generic acts mentioned in Appendix 3 there are others, listed below, that are more specific to the Health Service.

LEGISLATION
Access to Medical Reports Act 1988
Access to Health Records Act 1990 (largely replaced by Data Protection Act 1998)

SCOTTISH OFFICE POLICY DOCUMENTS
The principal Scottish Executive Letter & historical Management Executive Letters and SOHHD Circulars relevant to IT security are:

- CEL (2011) 25 Safeguarding Personal Data in Contracts
- CEL (2011) 26 NHS Scotland information assurance strategy
- CEL (2010) 31 Records management: NHS code of practice (Scotland)
- CEL (2008) 45 NHS Scotland mobile data protection standard
- CEL (2008) 13 Information sharing between NHS Scotland and the police
- HDL (2006) 41 NHS Scotland Information Security Policy
- HDL (2001) 1 The Use of Personal Health information, Submission of Records to Information Statistics Division, Disease Registers and The Confidentiality and Security Advisory Group for Scotland (CSAGS)
- MEL (2000)17 Data Protection Act 1998
- MEL (1999) 48 Manual for Caldicott Guardians
- MEL (1999) 19 Caldicott Guardians
- MEL (1996) 80 National IM and T programme board and strategy (including amendment MEL(1997) 01
- NHS Circular PCA (M) (1994) 11 Legitimisation of Patient Computer Records
- MEL (1992) 69 Access to NHS Health Records
- MEL (1992) 45 Computer Security Guidelines
- NHS/DGM (1992) 20 Security of Health Records
- NHS 1991 (GEN) 31 The Access to Health Records (steps to Secure Compliance & Complaint Procedures) (Scotland) Regulations 1991
- NHS 1991 (GEN) 27 Access to Health Records Act 1990 (Residual elements only as main elements incorporated into Data protection Act 1998)
- NHS 1990 (GEN) 22 Confidentiality of Personal Health Information – A Code of Practice
- SHHD/DGM (1987) 49 Disclosed information about Hospital Patients in the Context of Civil Legal Proceedings

Two Social Work Circulars may also be relevant:

- SW1/89 Confidentiality of Social Work Records
- SW2/89 Access to Personal Files/Regulations

There may also be other documents specific to each clinical discipline that need to be consulted and complied with. E.g., some may refer to electronic record retention periods, etc.