INFORMATION SECURITY POLICY

Release: Final
Reviewed: May 2019
Version 3.1

Compiled by: Stuart Hubbard, Information Manager
Document Reference: Information Security Policy v3.1.doc

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

TABLE OF CONTENTS

NHS SHETLAND DOCUMENT DEVELOPMENT COVERSHEET

Name of document	**Information Security Policy**		
Registration Reference Number	**HSPOL003**	**New** ☐	**Review** ☑
Author	**Stuart Hubbard**		
Executive Lead	**Lorraine Hall**		

Proposed groups to present document to:	
Information Support Group	
Clinical Governance Committee	

DATE	VERSION	GROUP	REASON	OUTCOME
5th November 2014	2.0	Information Support Group	PO	PRO
19th May 2015	2.0	Clinical Governance Committee	For Approval	Approved
12th September 2018	3.0	Information Governance	PO	Approved
27th November 2018	3.0	eHealth and Informatics Support Group (eISG)	PO	Approved
28 May 2019	3.1	Clinical Care and Professional Governance Committee	For Approval	Approved

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)

Version History

Date of this Version: September 2018

Date of Previous Versions:

Version	date	Summary of Changes	Changes marked
0.1		First draft.	No
1.0	14/10/2009	Final draft	No
1.1	01/03/2013	Planned refresh	No
1.2	06/03/2013	Minor revisions	No
2.0	05/11/2014	Separation of Information Security Policy from IT Security Policy	No
3.0	09/10/2018	Planned refresh. GDPR compliance	No
3.1	16/05/2019	Changes to Appendix B and review date and version front cover.	No

Overview

The purpose of information security is to ensure business continuity and manage risk by minimising the likelihood and impact of security incidents. Information security enables information to be shared while ensuring the protection of information assets.

Information takes several formats; it can be stored electronically, transmitted across IT networks, printed out or written down on paper. From an information security perspective, appropriate protection should be applied to all forms of information stored including paper-based information, computer databases, portable and fixed IT media and any other methods used to communicate information.

This policy sets out clear management direction and support for information security at NHS Shetland in accordance with business requirements, legislation, regulations, standards and guidance.

It demonstrates management support for, and commitment to, information security through issuing this policy for user acceptance and compliance, as well as any related policies, procedures and guidelines, including user education and awareness across NHS Shetland.

The purpose of this policy is to protect all NHS Shetland information assets from threats, internal or external, deliberate or accidental.

Applicability and Scope

Applicability

This policy applies to all information assets held by NHS Shetland and is intended to be fully consistent with the Information Security Policy and Standards of NHS Scotland.

This policy applies to all information assets, not just assets held electronically.

This policy applies to all users who undertake work for NHS Shetland or use any part of the IT infrastructure, whether as an employee, a student, a volunteer, a contractor, partner agency, external consultant or 3rd party IT supplier.

Scope

Information Security covers three main strands:

- Availability
- Integrity and
- Confidentiality

“Availability” means that the information is available to staff who need the information at the time and place that they require

“Integrity” means that the information that is retrieved from Information Systems is complete and accurate

“Confidentiality” means that information held is not available to staff who should not see the information

Management requires that all NHS Shetland information assets are properly safeguarded against breaches of confidentiality, integrity and availability.

To achieve this, the following attributes will at all times be in place with respect to matters relating to information assurance:

- Information Security Policy, objectives, activities and improvements will be aligned with the business objectives and organisational culture of NHS Shetland and meet the requirements of ISO/IEC27002, the Code of Practice for Information Security Management.
- A risk based approach to Information Security will be maintained enabling informed decisions on information security initiatives and ensuring that budget and resources are focussed appropriately. These security initiatives will meet the following objectives:
    - prevention of incidents via the identification and reduction of risks;
    - detection of incidents before damage can occur;
    - recovery from incidents via containment and repair of damage and prevention of reoccurrence.
- Information security will be promoted at all levels of the business through comprehensive user awareness education and training.
- Management will actively support information assurance initiatives, ensure they remain abreast of the risks to information assets and champion the continual improvement of information security at NHS Shetland.
- An effective Information Security Policy and corresponding security operating procedures will be maintained ensuring that:
    - all information assets are protected against unauthorised access and disclosure;
    - confidentiality of information will be assured at all times;
    - integrity of information will be maintained at all times;
    - business requirements for availability will be met;
    - breaches of security both actual and suspected are reported and investigated;
    - classification and ownership of information assets will be applied; and
    - regulatory and legislative requirements will be met, including compliance with the General Data Protection Regulation, Public Records Act and Access to Medical Records Act
    - Over and above legislative compliance, NHS Shetland strives to work to ISO 27001

Approach

Shetland NHS's approach to Information Security is defined by its Information Governance Policy. That policy is an overarching policy that defines a hierarchy of policies, of which the Information Security Policy is one. The relationship of the various policies, procedures and protocols is described in the Information Governance Policy; the diagram from section 5 of the Information Governance Policy is duplicated below to show the context of the Information Security Policy.

Approach for Individual Systems

The Information Security Policy defines in general terms how each individual information system must be governed. Each system must have

- An Access Protocol
- A Rapid Impact Assessment for Equality and Diversity
- A Data Privacy Impact Assessment
- An entry in the Information Asset Register
- An entry in the Data Flow Map

As appropriate, other documents may also be required, as directed by the eHealth and Informatics Support Group, potentially including

- A full Equality and Diversity Impact Assessment
- A Privacy Notice
- One or more Data Sharing Agreements

These documents together provide specific and explicit details that are pertinent to each individual system and together form, in effect, a set of standard operating procedures for the information system so that it delivers availability, integrity and confidentiality. The function of each of these types of document is described below.

Access Protocol

All information systems will have their own access protocol. The access protocol will describe the system, define which classes of staff will be able to do which kinds of transaction within the system, define how the system is administered, define how special accounts (for example, accounts used to identify and rectify faults) are operated and define how, when and for what purpose the system is audited. The access protocol will identify explicitly when data is shared between organisations. The access protocol will be signed off by the eHealth and Informatics Support Group in advance of the system implementation.

Equality and Diversity

All information systems will have their own rapid impact assessment for Equality and Diversity. This will consider if implementation of the system will have any effect on the Board's obligations regarding discrimination on any group of individuals; staff, patients, members of the public, volunteers, or any other identified group. Should the Information Support Group decide that there is an impact, then the Rapid Impact assessment will be replaced by a full Equalities and Diversity Impact Assessment.

Data Privacy Impact Assessment

All information systems will have their own privacy impact assessment. This document will consider if implementation of the system will impact on any individual's privacy. Should the impact assessment identify any privacy concerns the assessment will define processes and controls to minimise these concerns. The appropriate level of detail contained in the impact assessment will be determined by the Information Support Group. For example, Information Systems which relate to

patient information will require a more comprehensive assessment than systems which do not, more so if the information is shared between organisations, more so if the information is sensitive. The eHealth and Informatics Support Group will also decide on the level of consultation required. For example, an information system which does not relate to patient information may be signed off by the eHealth and Informatics Support Group without reference to external consultation, but patient information systems will require wider consultation with stakeholders, potentially including groups with patient representation.

Information Asset Register

The Data Quality Policy defines Shetland NHS's approach to data quality generally, but defines also how information system specific procedures are made. Details are contained within the Data Quality Policy but in brief, that Policy requires that an entry be made for the information system into the Information Asset Register and that a Data Quality procedure document be completed. Additionally technical support documentation for each Information Asset must be held in the System Catalogue. This includes server, software, security and support information and is aligned to the Information Asset Register via a common system identifier.

Privacy Notice

A Privacy Notice is a publically available document which describes to the public how their information is used and shared. The Information Support Group will decide if a privacy notice is required, and if so where it will be displayed and the extent of detail required.

Data Flow Map

NHS Shetland maintains a Data Flow Map which holds details of how different elements of information move through the organisation in order that an overview can be made on whether or not the system architecture is optimum. The data flow map extends beyond any single information system allowing consideration to be made how systems interact. The Map covers all systems, not just electronic systems and covers all interfaces between systems, not just electronic ones.

Data Sharing Agreement

If information passes from one organisation to another there must be a data sharing agreement which describes the process in detail. It must cover what data is shared, with whom, when, for what purpose and how the data will be safeguarded at the destination. Almost always there will be a companion Data Privacy Impact Assessment which will consider the implications for patients regarding the sharing of their data.

General approach for whole organisation

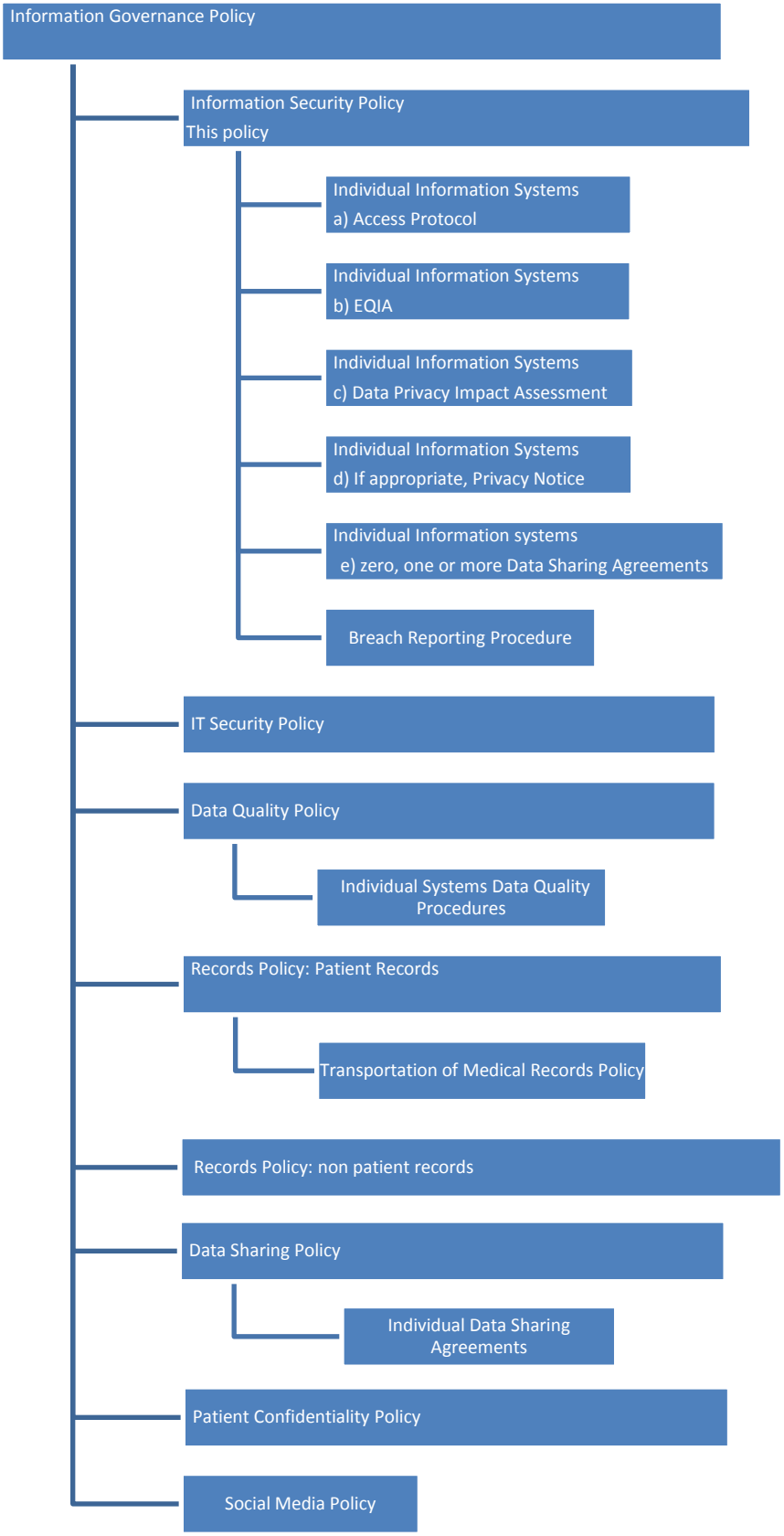
NHS Shetland will operate in accordance with its information security management system, ISMS. This will progressively align more and more closely with the ISO27000 suite of international standards. The alignment, and more specifically the

areas of non-alignment, will be monitored through a Information Governance Maturity Self Assessment. This self assessment will be monitored and updated regularly and the outcome reported to NHS Shetland management.

Breach reporting

The General Data Protection Regulation explicitly requires that all deviations from the Information Governance Policy are recorded in a Breach Register. Each breach will be considered to determine if it is necessary to report any particular issue to the Information Commissioner. The way that this is handled is described in the Breach Reporting Procedure.

Policy Map


Information Governance Policy
Information Security Policy
This policy
Individual Information Systems
a) Access Protocol
Individual Information Systems
b) EQIA
Individual Information Systems
c) Data Privacy Impact Assessment
Individual Information Systems
d) If appropriate, Privacy Notice
Individual Information systems
e) zero, one or more Data Sharing Agreements
Breach Reporting Procedure
IT Security Policy
Data Quality Policy
Individual Systems Data Quality Procedures
Records Policy: Patient Records
Transportation of Medical Records Policy
Records Policy: non patient records
Data Sharing Policy
Individual Data Sharing Agreements
Patient Confidentiality Policy
Social Media Policy

Responsibilities

The individuals and groups below have responsibilities under this Information Security Policy. They may have additional responsibilities, and additional individuals and groups may have responsibilities arising from other policies in the Information Governance portfolio, but these will be described in their own policy.

Chief Executive

Final responsibility for the secure operation of all systems used to process information in NHS Shetland is vested in the Chief Executive. This responsibility is delegated to all staff developing, introducing, managing and using information systems in accordance with this policy. The Chief Executive is ultimately responsible for accepting the residual risks evaluated by the information risk management process.

Caldicott Guardian (Medical Director)

The responsibility for protecting the confidentiality of patient identifiable information rests with the NHS Shetland Caldicott Guardian.

eHealth and Informatics Support Group

The NHS Shetland eHealth and Informatics Support Group (eISG) has the responsibility:

- To review and approve all Information Security policies. This includes this policy, the Information Security Policy, but includes also the companion policies and procedures described in the policy map on page 10.
- To oversee the deployment of the Information Security Management System.
- To maintain the Information Governance Maturity self assessment

Senior Information Risk Owner (Director of Finance)

The Senior Information Risk Owner (SIRO) is responsible for ensuring that:

- The Board is compliant with the Public Records Act and the General Data Protection Regulations
- Ensuring that NHS Shetland lodges a full, correct and up-to-date notification in its name with the Information Commissioner (MEL 2000 (17)).
- Reporting breaches in Information Security to the Information Commissioner.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for ensuring that:

- All of the policies and procedures relating to a particular information system are in place prior to implementation of the system and refreshed timeously.
- That policies and procedures relating to a particular information system are followed during normal operation
- A register of all NHS Shetland information assets is maintained. The register will record the data owners and identify those assets that are confidential or sensitive as defined in Data Protection legislation and Caldicott guideline.
- That the information asset register is kept up to date.
- A Data Flow Map for NHS Shetland is maintained
- A Document Register for NHS Shetland is maintained
- A Data Sharing Agreement Register for NHS Shetland is maintained
- A Record Deletion Register for NHS Shetland is maintained
- A Breach Register for NHS Shetland is maintained
- Advising on and monitoring data protection practices in NHS Shetland.
- Assisting the organisation with their responsibilities in relation to Data Protection.
- Undertaking regular audits of how personal information is handled is carried out.
- That audits are completed as specified in the access protocols.

Information Asset Owners

Each item in the Information Asset Register compiled by the Data Protection Officer (DPO) has an Information Asset Owner. The responsibilities attached to the Information Asset Owner will be concordant with the size and importance of the asset, but include at least:

- Liaising with the Data Protection Officer
- Maintaining the asset's Access Protocol

Functional, Service and Departmental Managers

Line managers are responsible for:

- Notifying system owners of changes to staff personnel so that access can be provided and withdrawn in a controlled and auditable manner.
- Ensuring that all current and future staff are appropriately trained
- Ensuring that no unauthorised staff are allowed to access any of NHS Shetland information systems.

- Determining which staff should be given authority to access specific information systems. The level of access to IT systems will be based on job function need, irrespective of status.
- Ensuring that their staff follow standard operating procedures in relation to the information system
- Appraising the Data Protection Officer when entries are to be added to or subtracted from the Information Asset Register, the Data Flow Map, The Data Sharing Agreement Register, the Document Register or the Record Deletion Register.

All Staff

All staff, including contractors and service providers, who influence the use of NHS Shetland information systems are responsible for:

- Conforming to the standards expected and described in this and any other associated information security policies.
- Reading and 'signing up' (accepting) to this and any other relevant information security policies which are relevant to their job role.
- Complying with specific information security responsibilities required of them as defined in their job description and also within information systems secure operating procedures documentation.
- Taking personal and professional responsibility for dealing securely with any information they have access to in the course of their duties.
- Ensuring their actions when using these assets fully conform to this and related policies, NHS Scotland standards and legal requirements.
- Ensuring that no breach of Information security results from their personal actions. This is also equally applicable for staff authorised to access and use NHS Shetland Information systems remotely.
- Fully complying with all NHS Shetland Information Security Policies, Standards and Procedures.
- Notifying their Line Manager of all suspected or actual breaches of Information security.

Failure to observe this policy may result in disciplinary action or legal proceedings being taken. Standard supplier contracts will also require contractors and other third parties to comply fully with the provisions of this and other NHS Shetland Information Security policies.

Operational systems

Confidentiality of Information Systems

This will be maintained by ensuring that:

- Only authorised NHS Shetland staff and NHS Shetland partners will be granted access to information systems and that access will be restricted to the information required for the person's job function i.e. only on a *need to know* basis
- Where staff outwith NHS Shetland are granted access to NHS Shetland Information Systems an agreement must be in place between NHS Shetland and the third party which covers appropriate use of the system, the audit in place to monitor their use and action to be taken in the event that audit reveals inappropriate use.
- Where multiple staff share access to a NHS Shetland Information System, each member of staff will be provided with a unique identifier. All transactions on such systems must be attributable and auditable to the user who conducts the transactions. In circumstances where such systems do not provide an auditable trail of use, measures should be put in place to manually audit user transactions.
- Passwords must be defined in line with national NHS Scotland standards and kept confidential at all times.
- Access to NHS Shetland information systems from external IT networks and other types of communication link will only be permitted on an exception basis and be subject to an additional layer of security, in line with national and NHS Scotland remote connectivity standards and regulations.
- NHS Shetland controls and monitors internal access to external networks and reserves the right to disconnect immediately, and if necessary, permanently, any member of staff or organisation attempting to breach this or any other NHS Shetland Information Security Policy.

Integrity of Information Systems

This will be maintained by ensuring that:

- All Information Systems will have a completed Data Quality procedures document completed.
- All NHS Shetland information assets will operate in accordance with Information systems manufacturer specifications.
- Updating and other activities that could affect the integrity of information must be restricted to authorised staff needing to do so as part of their job function, in line with Caldicott principles on access to confidential information.
- Training will be available in all information systems

Availability of Information Systems

This will be maintained by ensuring that:

- Access requests for accounts in Information Systems are processed timeously
- Regular backups are taken of all IT systems and stored in a secure manner along with trial restorations.
- Business continuity / disaster recovery plans are in place.

System Development

Staff who authorise the development or purchase of information systems will be responsible for ensuring that the specification conforms to the purpose for which the systems are required. Developers or procurers of information systems, including service providers, will be responsible for ensuring that systems produce results as specified and provide adequate levels of availability, integrity and security.

Compliance

NHS Shetland staff will comply fully with all relevant legislation and give consideration to advisory instructions from NHS Scotland and the Scottish Government. A list of the principal legislation and formal administrative guidance on information security with which NHS bodies must currently comply is provided in Appendix A.

In particular:

- The NHS Shetland Internal Audit function will review and report at defined intervals upon controls and security levels which operate at a system and application level. Specifically, Internal Audit will report upon the compliance of NHS Shetland with this policy.
- NHS Shetland is required to make arrangements for adequate levels of audit to be undertaken.

Risk Management and Business Continuity

NHS Shetland will complete risk assessment and management documentation for all information systems to ensure that threats and vulnerabilities are identified and risk is minimised through the application of balanced security controls.

NHS Shetland will ensure suitable disaster recovery and contingency arrangements are in place.

Recovery procedures will be developed for all IT operational systems and, where relevant, appropriate contingency plans will be documented and tested to ensure an acceptable level of service and control is maintained following a system failure.

Policy distribution

The Information Security Policy and all subsequent associated policies will be communicated to all members of staff in NHS Shetland and to any appropriate third-party individuals or companies working on behalf of the organisation.

Review

This Policy will be reviewed at appropriate intervals if appropriate to take into account changes to legislation that may occur, and or guidance from the Scottish Government and or the UK Information Commissioner. The review will be conducted in line with existing NHS Shetland procedures.

Appendix A

The Principal Acts of Parliament and Scottish Government circulars relevant to this policy are:

- CEL (2008)45 NHS Scotland Mobile Data Protection Standard
- SGHD HDL (2006) 41
- SGHD MEL (1993) 59
- MEL 2000 (17) Data Protection Act 1998
- Scottish Government Records Management: NHS Code of Practice (Scotland) January 2012.
- Public Records (Scotland) Act 2011
- Computer Misuse Act 1990
- Data Protection Act 1998 and updated by the General Data Protection Legislation, formally the Data Protection Act 2018
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Appendix B

Staff members holding the principle Information Governance Roles as of May 2019:

Chief Executive	Simon Bokor-Ingram
Caldicott Guardian	Brian Chittick
Senior Information Risk Owner (SIRO)	Colin Marsland
Data Protection Officer (DPO)	David Morgan

A continuously updated and more comprehensive version of this list is published at: https://intranet.nhsshetland.scot.nhs.uk/corporate/ig/index.html