



Corporate Information Security Policy

IGP04 2016

Corporate Information Security Policy

Version 4.1

Frank Rankin

Information Governance Manager

NES Digital

frank.rankin@nes.scot.nhs.uk



© NHS Education for Scotland 2016. You can copy or reproduce the information in this document for use within NHSScotland and for non-commercial educational purposes.

Use of this document for commercial purposes is permitted only with the written permission of NES.

Contents

3

| | |
|---|----|
| Objective..... | 4 |
| Scope & Applicability..... | 4 |
| Responsibilities..... | 6 |
| Information Security Management System..... | 12 |
| Information security risk management..... | 14 |
| Information Security Objectives 2016-29 | 16 |
| Operational Systems and Information Assets..... | 17 |
| Implementation of Information Security..... | 19 |
| Mobile Devices, remote access and homeworking | 21 |
| Systems Development..... | 22 |
| Authentication and registration of users..... | 24 |
| Security of third party access..... | 26 |
| Security classification..... | 28 |
| Legislation and standards..... | 29 |
| NHS Scotland guidance frameworks | 30 |

Objective

The objective of this policy is:

- to ensure the Confidentiality, Integrity and Availability of all NES information assets
- to protect NES information assets from threats, internal or external, deliberate or accidental, and
- to reduce information risk by reducing the likelihood and/or impact of information security incidents.

This policy sets out clear management direction and support for information security at NHS Education for Scotland (NES) in accordance with business requirements, legislation, regulations, standards and guidance. [\[ISO/IEC27001:2013 5.2\]](#)

NES is committed to satisfying the requirements of ISO/IEC27001:2013 and the NHSScotland Information Security Policy and guidance in meeting its information security objectives. [\[ISO/IEC27001:2013 5.2c\]](#)

Scope & Applicability

The policy applies to information in any format or medium held on NES premises, equipment and infrastructure, on cloud or other hosted environments, or held by NES employees or third parties on behalf of NES.

This policy applies to all users who undertake work for NES 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.

All NES information assets must be properly safeguarded against breaches of confidentiality, integrity and availability.

To achieve this, the following measures will be in place with respect to matters relating to information assurance:

- 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 NES.

- Information Security Policy, objectives, activities and improvements will be aligned with the business objectives and organisational culture of NES and meet the requirements of ISO27001.
- 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
 - Where possible, detection of incidents before damage occurs
 - 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 appropriate user awareness education and training
- An effective Information Security Policy and procedural environment will be maintained ensuring that;
 - Regulatory and legislative requirements are met, including compliance with the Data Protection Act 1998, EU General Data Protection Regulation 2016 and any successor legislation **[ISO/IEC27001:2013 18.1.1]**
 - All information assets are protected against unauthorised access and disclosure
 - Confidentiality of information will be assured
 - Integrity of information will be maintained
 - Business requirements for availability are met as far as possible
 - Breaches of security both actual and suspected are reported and investigated
 - Ownership of information assets is identified and recorded.
[ISO/IEC27001:2013 8.1.2]

Responsibilities [ISO/IEC27001:2013 6.1.1c]

Final accountability for the secure operation of all systems used to store information assets in NES is vested in the **Chief Executive**. This responsibility is delegated to all staff developing, introducing, managing and using information systems throughout the medium of this policy. The Chief Executive will ensure that:

- A NES-wide information security management system is established that integrates effectively into other relevant functions.
- Resources needed for the effective operation of the ISMS are available and is supported by Executive Group.
- A NES-wide information security policy is established, appropriate to the needs of NES and aligned with the NHSS information security policy framework.
- The role of senior information risk owner (SIRO) is assigned at executive level to ensure that the above is undertaken and performance on the ISMS reported to senior management at regular intervals.
- All the above is communicated to staff, business partners and the wider public to ensure that trust and confidence is maintained.¹

The **Director of the NES Digital Directorate** has operational responsibility for all aspects of information governance, including information security arrangements and is the designated **Senior Information Risk Owner**.

The responsibility for overseeing the adequacy of NES arrangements for maintaining the confidentiality of patient identifiable information rests with the NES **Caldicott Guardian**.

[ISO/IEC27001:2013 18.1.4]

The **NES Operational Leadership Group** has the responsibility to review and approve user-focussed Information Security guidance and protocols. [ISO/IEC27001:2013 5.1.2c]

The **Senior Information Risk Owner** has the responsibility to review and approve corporate or technically-focussed Information Security policies.

¹ NHS Scotland Information Security Policy 2015, section 1

The **Director of the NES Digital Directorate** has the responsibility to ensure that:

- NES IT infrastructure, development and service delivery practice supports and enables all relevant Information Security policies to be implemented.
- NES Digital Directorate staff work within a clear information security framework which is documented and regularly reviewed.

Corporate Digital Services has the responsibility to ensure that:

- As far as possible, IT systems and assets are held in secure areas that provide protection from unauthorised access and environmental threats such as fire, flood and loss of power and that relevant risks are registered and managed.
- All information assets are securely removed before equipment is re-allocated or sent for secure disposal/destruction under contract by an authorised recycling service.
- Protection against malicious code is operating on all networked devices, workstations, servers and data exchange systems.
- Incoming data (including data held on IT media, e-mail and Internet downloads) is scanned for malicious code before installation or use.
- Back-up and recovery procedures are in place and tested.
- The recording and monitoring of interaction with external IT systems is supported as required.
- All technical and procedural controls mandated under this policy are timeously and effectively implemented.
- Ensuring 3rd party connections comply with the Scottish Wider Area Network code of connection
- Provide appropriate assistance, advice and access to the Information Governance Manager to facilitate the monitoring and audit of systems and processes.

Third Parties

NES and external organisations need to share information with each other and, in some cases, allow access to IT resources. Information sharing brings with it increased risk to the security of the data and the systems on which it is held. Before allowing third party access to NES networks, a **risk assessment** will be carried out by the Director of the NES Digital Directorate to establish the level of risk and to identify any necessary counter-measures before access can be authorised.

Access to information assets by third parties will only be allowed when the appropriate security measures have been implemented and an agreement has been signed defining the terms for the data sharing. **[ISO/IEC27001:2013 8.1.3]**

Any trusted third party with direct access to NES systems is responsible for compliance with this policy and any other relevant policies and procedures and must only access information within the terms of their authorisation and only for the purposes and tasks agreed by NES.

Cloud Service Providers contracted by NES to provide infrastructure, platform or software as a service will be responsible for:

- Maintaining the security of the Cloud services to current industry standards and best practice, including the UK Government Cloud Security Principles and the Cloud Security Alliance Cloud Control Matrix
- Providing NES with reporting, monitoring and audit information and opportunities, adequate for NES to be assured of the security of our assets and systems.
[ISO/IEC27001:2013 8.1.3c]
- Providing evidence to NES of current independently certified compliance in their business processes against ISO27001:2013.
- Providing advice and support to NES on our responsibilities as service users in maintaining the security of the Cloud services and assets.
- Compliance with any contract terms or data processing agreement terms placed on them by NES.

The **Information Governance Manager** is the designated data protection officer and will ensure that:

- A register of NES corporate information assets is maintained. The register will record data owners and designate those assets that are confidential or sensitive as defined in Data Protection legislation and Caldicott guidelines. [ISO/IEC27001:2013 8.1.2]
- Queries about handling personal information are promptly dealt with.

The Information Governance Manager is also the information security officer responsible for the maintenance of the Information Security Management system and for advising, monitoring and reporting on the implementation of and compliance of all Information Security Policies. This includes but is not limited to:

- Ensuring that the Information Security Policies are promoted and implemented throughout NES;
- Assisting asset owners to determine the level of security required for new information systems or assets;
- Assisting asset owners in conducting risk assessments on information assets;
- Reporting on the state of information security within NES to management and, where appropriate, to internal stakeholders and external authorities (Scottish Government and the Information Commissioner's Office); [ISO/IEC27001:2013 6.1.3c]
- Promoting compliance with relevant legislation and NHS Scotland Information security guidance;
- Raising staff awareness of their responsibilities and accountability for information security;
- Monitoring, recording, escalating and reporting actual or potential information security breaches, including reports to NHSScotland, Scottish Government and the Information Commissioner where necessary.

Information Asset Owners are senior managers who have been identified as having primary responsibility for one or more corporate information assets. They have the following responsibilities:

- Ensuring that systems under their authority have appropriate security policies in place;
- Ensuring that staff with access to the systems under their authority are aware of their responsibilities for maintaining the integrity of those systems;
- Ensuring that any contracts, service level agreements or other outsourcing arrangements with third parties to provide systems or services affecting the asset contain appropriate information governance clauses and instructions;
- Providing assurance to the Senior Information Risk Owner regarding the management of information risk affecting their information asset(s).
- Advising the Information Governance Manager of significant changes to the information systems and assets under their authority.

Line Managers have the following responsibilities:

- Managers will notify the Digital Directorate immediately of changes to staff personnel so that IT access can be provided and withdrawn in a controlled and auditable manner;
- Managers will notify the administrators of corporate systems (such as risk, project or performance management, portals or training databases) of any relevant changes to staff personnel so that system access can be provided and withdrawn in a controlled and auditable manner;
- Managers will ensure that all current and future staff are trained in their personal information security responsibilities, appropriate to their role;
- Managers will ensure that any staff who use IT systems/media are trained in their secure and appropriate use;
- Managers will ensure that no unauthorised staff are allowed to access any of NES IT systems;

- Managers will determine which staff should be given authority to access specific IT systems. The level of access to IT systems will be based on job function need, irrespective of status;
- Managers will implement procedures to minimise NES exposure to fraud/theft/disruption of its IT and information assets;
- Managers will ensure that key documentation is maintained for all critical job functions to ensure Departmental business continuity in the event of staff unavailability.
- Line Managers will ensure that staff handling personal information understand that they are contractually responsible for following good data protection practice and are appropriately trained to do so.
- Managers will ensure that staff receive training appropriate to their roll and complete any required mandatory Information Governance training.

The **Human Resources Directorate** will ensure that:

- Adequate background checks are carried out on applicants for employment with NES, appropriate to the role and in compliance with current NHSScotland guidelines.
- All employment contracts contain appropriate terms for confidentiality and information security.

All Staff

All staff entrusted with access to NES information assets have a responsibility to ensure that their actions fully conform to this and related policies, NHSScotland standards and legal requirements as set out in the NES User Information Security Policy.

Any NES employee who develops or acquires an information system has a responsibility to ensure they notify and register the system with the Information Governance Manager before the system is made operational. In addition, the authority to conduct this work must be sanctioned by the Director of the NES Digital Directorate in the first instance.

Information Security Management System

NES shall maintain an Information Security Management System, the scope of which shall be all staff of the Digital Directorate and all assets and services managed or delivered by the Digital Directorate. [ISO/IEC27001:2013 4.3]

NES is committed to continual improvement of the ISMS through regular management review and the audit process. [ISO/IEC27001:2013 5.2d] The SIRO-chaired Top Management Group will conduct a management review of the ISMS at planned intervals to ensure its continuing suitability and effectiveness. This will be measured against the NES and NHSS Information Security Policy Framework. Such review will include consideration of:

- Status of actions from previous management reviews.
- Changes in external and internal issues which are relevant.
- Non-conformities in the ISMS and preventative/corrective actions.
- Monitoring and measurement of results.
- Audit results.
- Results of high-level or significant risk assessment and risk treatment plans.
- Feed-back from interested parties including patients.
- Significant security incident reports at Board and national level.

The outputs of the management review shall include decisions related to continual improvement, opportunities and any changes needed to the information security management system. [ISO/IEC27001:2013 9.1, 5.1]

NES Digital Directorate will respond appropriately when nonconformity is identified - over and above any regular audit and management review - and act to deal with it including change to the information security management system.

NES recognises the circular nature of the ISMS: to plan, do, check and act to achieve continual improvement.²

² IG4 NHS Scotland Information Security Policy Framework 2015-17, s 9

The Information Security Officer will ensure that NES shall conduct internal audits³ at planned intervals that provide information on whether the ISMS conforms to the requirements of ISMS as planned and implemented. The audit shall:

- Work per an agreed frequency (e.g. annual).
- Define the scope of the audit and criteria.
- Be carried out by colleagues who are qualified, objective and impartial.

Where appropriate, the IS audit activity will operate in liaison with the internal audit function.

³ NHS Scotland Information Security Policy 2015, section 8

Information security risk management

NES will adopt and consistently apply an information security risk treatment process that:

- Selects appropriate information security risk options for the information risk assessment results.
- Determine all the controls that are necessary to treat the information security options.
- Ensures that all the Reference control objectives and control types cited in ISO-27001 are considered and verify that none have been omitted.
- Ensures that the relevant NHSS National-level mandatory controls and standards are implemented including that of the Scottish Wide Area Network (SWAN).
- Ensures that significant incidents are reported as per national policy so that lessons learned reports feed into treatment plans.
- Ensures that the formal process of NHSS national accreditation is followed regarding systems/services that require it. It is the responsibility of the Board(s) or other organisations using the systems/services to complete the risk management and accreditation document set for the NHSS-wide accreditor.
- Considers all controls in NHSS National Guidance and implement as far as practicable.
- Considers all the controls cited in ISO27002
- Produces a statement of applicability that contains the necessary controls and justification for inclusions, exclusions and whether implemented.
- Considers any other control objectives and types over and above those in ISO-27001/2 that have applicability to the Board.
- Formulates an information security risk treatment plan.
- Obtains the risk owners' formal approval of the information security risk treatment plan and acceptance of the residual information security risks. Where non-NHSS organisations and suppliers are involved the Board shall seek agreement on which party is responsible for discharging the different components of the treatment plan.

NES will implement the agreed information security treatment plans and retain document evidence.⁴

⁴ IG4 NHS Scotland Information Security Policy 2015, section 6

The NES information security risk assessment process will apply the current NES Corporate Risk Management strategy to information assets and processes.

[ISO/IEC27001:2013 6.1.2]

The Information Security Manager will maintain a Statement of Applicability (SOA) based on the controls set out in ISO27002:2013 and current NHSScotland policy⁵

Information risk assessments will be carried out on a corporate basis by the Information Security Manager against the areas identified in the SOA, and will be reviewed on an annual basis. Where changes to information processes or assets present new specific areas of risk, the Information Security Manager will assist Information Asset Owners in carrying out a risk assessment.

The identified risks and controls and the risk treatment plan (actions) will be recorded in the NES risk management system, the [Integrated Planning and Performance System \(IPPS\)](#), as Project-level risks, cross-referenced to the SOA. The risk treatment plan within IPPS will be approved by the Senior Information Risk Owner and Top Management Group on an annual basis. **[ISO/IEC27001:2013 6.1.3]**

⁵ IG4A NHS Scotland Information Security Framework Annex of Controls, 2015

Information Security Objectives 2016-29

NES shall establish high level information security objectives for the entire organisation.

These shall be aligned with:

- NHSS eHealth Strategy, so that the Information security function and ISMS support all seven strategic aims.
- NHSS/SG Information Governance Improvement Plan.
- The set of specific, measurable actions relating to information security to be undertaken at national level over a defined period as part of NHSS eHealth Programme.
- NES- specific actions that need to be undertaken, the planning, resources, time-scale, persons responsible and how/when results to be evaluated.⁶

NES will have the **following objectives** for the ISMS **[ISO/IEC27001:2013 6.2]**:

- NES will have no information security incidents with an impact higher than “Minor” during 2016-2018.
- Fully implement July 2015-issued NHS Scotland Information Security Policy Framework by April 2017.
- Maintain and improve information security during Cloud migration, achieving ISO27001:2013 certification for NES cloud-based services during 2017.

⁶ NHS Scotland Information Security Policy 2015, section 2.

Operational Systems and Information Assets

Confidentiality of systems and information assets will be maintained by ensuring that:

- All NES staff and contractors are subject to confidentiality clauses in employment and procurement contracts.
- Only authorised NES staff (including temporary and seconded staff) and contractors will be granted access to information systems. Prior management authorisation must be obtained before equipment, information or software is removed from NES sites. **[ISO/IEC27001:2013 11.2.5]:**
- For highly sensitive (Category Red) data and documents, specific restrictions may be added to the site, folder or system.
- For access to NES information systems, each member of staff will be provided with a personal authentication identity. All transactions on such systems must be attributable and auditable to the user who conducts any transactions.
- Passwords must be defined in line with national NHSScotland standards and kept confidential.
- NES will provide managed web-enabled access to selected systems through Web services on a risk-assessed basis. Any other access to NES information systems from external networks and other types of communication link will only be permitted on an exception basis and will be subject to an additional layer of security, in line with national and NHSScotland remote connectivity standards and regulations.
- NES will control and monitor internal access to external networks and reserves the right to disconnect immediately, and if necessary, permanently any network connection involved in a breach of this or any other NES information security policy.
- NES will operate a clear desk policy. Staff must ensure that mobile computing devices and paper files or other media containing personal or sensitive information, are locked securely away when not in use.

- Staff must ensure that work stations are locked whenever they leave their desk.

Integrity of systems and information assets will be maintained by ensuring:

- All NES Information assets will operate in accordance with IT systems manufacturer specifications.
- Information Asset Owners will apply appropriate controls, checks, quality assurance processes and staff training to ensure the integrity and quality of data within the asset.

Availability of systems and information assets will be maintained by ensuring:ISO27001:2013 12.3.1

- Regular replications and/or backups are taken of all information systems and stored in a secure manner.
- Network servers are replicated at least once daily to a partner site and backed up after each working day in line with the Corporate Digital procedures.
- Backups are tested regularly to ensure that systems/files can be restored when required.
- Business Continuity/Disaster recovery plans are in place for all NES sites.

Implementation of Information Security

Documentation of procedures

Digital Directorate IT operating procedures should be documented and made available to all colleagues who need them.

The approved methods for recording and making available documented operating procedures are as follows:

- Digital Procedure documents in MS Word or PDF format stored within the Digital Directorate site in SharePoint Online
- Procedure documents stored within the designated area of OneDrive for synchronisation to the laptops of relevant team members
- The Secure Development Lifecycle Wiki page in SharePoint Online
- Knowledge Base entries within Service Now

Segregation of duties **ISO27001:2013 6.1.2**

NES will maintain the principle of segregation of duties to reduce the risk of misuse of information assets. Appropriate measures will be taken to ensure as far as possible that no single person can modify systems or assets without authorisation or detection. Measures will include:

- Initiation of a technical change event will be separate from authorisation (see change control procedures)
- Monitoring and logging (see below)
- Wherever the specific system permits, linking administrative rights to individual accounts, avoiding generic administration accounts.

Information security in project management ISO27001:2013 6.1.5

NES will address information security in the management of all relevant projects, whether technical, business or educational.

For development projects, the Microsoft Secure Development Lifecycle for Agile approach is integrated into the project management methodology.

For Corporate Digital Services, major projects, the Office 365 Planner app will be used to ensure an audit trail of all tasks, updates and actions taken.

For all other projects, project owners are required to consult the Information Governance team for advice on information security and privacy issues, risk-assessment and treatment.

Separation of development, testing and operational environments

NES Digital Directorate shall have appropriate separation between the technical environments where applications are developed/configured and tested and the live production environment.

For cloud based software-as-a-service, this separation is enforced by the provider.

For NES Development Teams see the Secure Development Lifecycle Wiki for further details of environment separation.

For on-premises software, the building and testing of applications carried out by the infrastructure and client technologies functions of Corporate Digital Services will be in development environment separate from the live production environment managed by client technologies.

Mobile Devices, remote access and homeworking

This policy applies in situations where NES deploys mobile computing devices which have been purchased by NES and to authorised business use of employees' personal devices.

Mobile devices present a risk due to the increased potential for theft or loss. NES will manage the risks associated with the use of mobile devices and media in line with the eHealth guidance set out in *Managing Information Assurance for mobile wireless services in NHSScotland: Good Practice Guide* (May 2012).

Where authorised by line management, staff may use personal devices to access and manage non-sensitive NES data in compliance with the controls and processes set out in the User Information Security Policy.

Staff may work with NES data in a home or non-office environment in compliance with the User Information Security Policy, homeworking and teleworking policies.

[ISO/IEC27001:2013 11.2.6]:

Systems 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 external service providers, will be responsible for ensuring that systems produce results as specified and provide adequate means of security. The relevant security requirements for a system must be documented and included in the specification for any new or significantly changed system. [ISO/IEC27001:2013 14.1.1]:

NES development teams will apply the Microsoft Secure Development Lifecycle to development projects, suitably adapted for NES purposes. This provides secure engineering principles for development of applications. [ISO/IEC27001:2013 14.2.1 and 14.2.5]:

New information systems being considered for procurement by NES must include adequate security measures that are clearly assessed and documented in the Business Case. The regulatory framework of the NHS, including Data Protection and Caldicott requirements must be adhered to, both in the requirement, design and implementation stages.

The testing of all applications must be documented and attention paid to all aspects of security. Configuration Management must be used for each system – specifically, all initialisation files, data and test results files and system files must be identified and preserved with appropriate security and accountability. [ISO/IEC27001:2013 14.3.1]

Operational data will not be provided for use in application development or testing outside of NES own secure IT environment. Any personally identifiable data to be used for testing must be obfuscated (false identifiers added to genuine user data) before use in test or development environments. [ISO/IEC27001:2013 18.1.4]

In provisioning databases on a cloud platform, NES will apply EU-only data replication options. Any exception will be managed on an individual basis with the justification and all additional controls or risk assessment documented. In the configuration of firewalls, NES

will adopt Microsoft Development Network best practice. Server certificates are mandatory for all servers with external connections and recommended for internal-only servers.

NES will apply encryption in transit for all application data and communications, implementing Transport Layer Security (TLS) wherever possible [ISO/IEC27001:2013 14.1.2] including the use of opportunistic TLS for email traffic. [ISO/IEC27001:2013 13.2.1

NES will apply encryption at rest (SQL TDE) by default for all databases. Any exceptions to the TDE setting will be justified and documented.

Any system designed to be accessible on mobile devices and which provides access to personal or other sensitive data must ensure that no data is cached or saved to devices or that data is removed from those devices once the service or connection has terminated. ([See eHealth Mobile Device Guidance 2012](#)).

Authentication and registration of users

([ISO/IEC27001:2013 9.3.1c])

The identification and authentication of authorised users of NES systems is core to effective information security.

Line managers are responsible for informing Digital Directorate and the administrators of other relevant systems at the earliest opportunity of all new users (joiners), moving staff and leavers, indicating what information assets and level of authority they should have. Line managers must also inform Digital Directorate and the administrators or any other relevant systems of any changes to the required level of access and authority. Digital Directorate and system administrators will maintain document procedures for the registration and removal of users.

Users of all systems are responsible for ensuring that their passwords are kept secure and confidential. Under no circumstances, shall users write down their passwords or share them with other users, including Director of the NES Digital Directorate staff.

If a user suspects that someone else may have become aware of his/her password (for instance, if another person has watched the user enter the password), the user must immediately change his/her password. If they believe NES systems or data have been compromised they must log an incident with the Information Governance Manager for investigation.

System administrators will, where technically possible, configure password requirements on NES systems as follows: **([ISO/IEC27001:2013 9.4.3])**:

- be a minimum of 8 characters in length; where possible, the minimum character length will be configured in the system;
- force a change at least every 90 days;
- enforce password history of 6;
- be changed on first login;
- contain at least three of the four possible character types, (lowercase letters, upper case letters, numbers and special characters);

No member of NES Digital Directorate staff will ever need to ask for a user's password and users must never disclose a password to anyone.

Third Party support staff must be issued with their own unique ID and password to carry out their tasks. Upon completion of the agreed work the account must be disabled. The account shall only be re-enabled when third parties have further approved work to complete.

Security of third party access

[ISO/IEC27001:2013 13.2.4]

No external agency (NHS or not) will be given access to any NES networks unless the access has been formally authorised. All access by non-NHS agencies will be governed by contracts which will include security and confidentiality agreements. External agencies will only be allowed access to specific/relevant systems. NES will control all external agencies' access to its systems via SWAN remote access for organisations that have full code of connection.

Where this is not possible then access using similar standards (such as strong authentication and VPN) may be used as an alternative. Any third-party access to NES systems will be subject to risk assessment as appropriate.

[ISO/IEC27001:2013 15.1.1, ISO/IEC27001:2013 15.1.2, ISO/IEC27001:2013 15.1.3]

Contractual arrangements with third parties will include agreement on the classification of information, the need for confidentiality control and how this will be applied. Where confidential information is to be (or could be) accessed, NES will require any supplier to have formal contractual confidentiality clauses with all employees accessing such data. Where the third party is processing personal data (relating to identifiable individuals) on behalf of NES, their work shall be subject to a Data Processor Agreement.

[ISO/IEC27001:2013 18.1.4]

Contractual and other agreements between NES and third parties accessing our systems or information assets should include the following wherever appropriate:

- Authorised means of connection.
- Controls over return/destruction of information. [ISO/IEC27001:2013 8.1.4]
- Agreement on acceptable levels of data integrity and availability.
- Liabilities of the parties to the agreement.
- Legal responsibilities (Data Protection, Intellectual Property etc.).

[ISO/IEC27001:2013 18.1.2]

- The right to revoke agreement or access by any party in particular circumstances.
- The right of NES to receive and examine evidence of compliance from the third party.
- Protection against malicious software.
- Arrangements for reporting and investigating potential breaches including full audit trails.
- Involvement with additional subcontractors.
- Authorisation and authentication processes for Users.

Security Classification [ISO/IEC27001:2013 8.2.1]

NES has adopted the NHSScotland Green, Amber, Red classification of information:



| eHealth Guidance | NES examples | Equivalent UK Government Security Classification |
|--|---|---|
| <p>GREEN: Unclassified information</p> <p>This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.</p> | <p>Most NES documents fall within this category, including:</p> <ul style="list-style-type: none"> Names, posts of trainees Most management correspondence and minutes Work contact details | OFFICIAL |
| <p>AMBER: Protected information</p> <p>In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:</p> <ul style="list-style-type: none"> Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost. Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result). Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments). | <ul style="list-style-type: none"> Information on the performance or health of individual colleagues or trainees Commercially sensitive procurement information during the tendering process Home contact details Sensitive management discussion | OFFICIAL |
| <p>RED: Highly sensitive information</p> <p>Most boards also hold some information which is highly sensitive. Particularly:</p> <ul style="list-style-type: none"> Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health. Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). Information relating to vulnerable persons' health (e.g. child protection cases) Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc. | <ul style="list-style-type: none"> Detailed E&D information identifying individuals, particularly sexual orientation Serious allegations against individual trainees Banking or credit card details of individuals | <p>OFFICIAL – SENSITIVE PERSONAL</p> <p>When communicating with UK or Scottish Government agencies, local authorities or the Police, Red data must be labelled as OFFICIAL – SENSITIVE PERSONAL.</p> <p>[ISO/IEC27001:2013 8.2.2]</p> |




Legislation and standards




| Source | Title | Link |
|--------------------------------------|---|---|
| International Standards Organisation | ISO/IEC27001: 2013 Information Security Standards | |
| International Standards Organisation | ISO15489 Records Management Standard | |
| Legislation | Computer Misuse Act 1990 | http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm |
| Legislation | Freedom of Information (Scotland) Act 2002 | http://www.opsi.gov.uk/legislation/scotland/acts2002/20020013.htm |
| Legislation | NHS Education for Scotland Order 2002 | http://www.opsi.gov.uk/legislation/scotland/ssi2002/20020103.htm |
| Legislation | Data Protection Act 1998 | http://www.opsi.gov.uk/acts/acts1998/19980029.htm |
| Legislation | European General Data Protection Regulation 2016 | |
| Cabinet Office, UK Government | Cloud Security Principles | https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles |
| Cloud Security Alliance | Cloud Controls Matrix | https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ |
| SGD eHealth Directorate | eHealth Mobile Device Guidance | http://www.sehd.scot.nhs.uk/mels/CEL2012_25.pdf |


[Regulatory Framework Tracker](#)





NHS Scotland guidance frameworks



| | |
|---|--|
|  | <h2>Information security policies</h2> <p>Strategy level</p> <p>The eHealth Strategy 2014 – 2017 (2014) The eHealth Infrastructure Strategy (v1.1 August 2013) The eHealth Application Strategy (v1 June 2012)</p> <p>Information Governance</p> <p>Director Letter Information Governance (2015) IG1 Information Governance one page executive briefing April 2015 (2015) IG2 Information Governance Improvement Plan April 2015 (2015) Caldicott Guardian Manual The Information Governance Review (“Caldicott 2”) (March 2013) CMO Scotland response to The Information Governance Review (June 2013)</p> <p>Information Security</p> <p>IG3 Introduction NHSS Information Security Policy April 2015 (2015) IG4 NHSS Information Security Policy Framework (2015) IG4A NHSS Information Security Policy Framework ANNEX of Controls (2015) Security Classification Framework – impact on eHealth (Feb 2014) BMA Guidance on Use of Social Media (2012)</p> |
|  | <h2>Organisation of information security</h2> <p>NHS Scotland docs</p> <p>Information Assurance Advice to NHS Boards (2011) Board Information Security Policy (Template, e-library, v1.1, June 2010) Revised mobile data standard (SG eHealth, 2012) Mobile device guidance (SG eHealth, 2012)</p> <p>External docs</p> <p>Resource page for mobile device security (Apple, Android, Windows, etc.) (On NHS Scotland Information Security site)</p> |

| | |
|---|--|
| | <p>Remote Access (HSCIC v2.0 July 2009)</p> <p>Use of Tablet Devices in NHS environments (HSCIC 2011)</p> |
|  | <h2>Human resources security</h2> <p>NHS Scotland docs</p> <p>Handling Information Securely – a Guide for NHS Staff (Feb 2016)</p> <p>PIN Safer Pre and Post Employment Checks (Policy for NHS Scotland, 2014)</p> <p>NHSScotland information security good practice guide – for staff (e-library, final version, Dec 2008)</p> <p>Information security posters/screensavers (this site, 2010)</p> <p>External docs</p> <p>Pre-employment screening GPG (CPNI v3.0 May 2009)</p> |
|  | <h2>Asset management</h2> <p>NHS Scotland docs</p> <p>NHS Scotland Information Classification Scheme (2015)</p> <p>Records Management: NHS Code of Practice v2.1 (2010)</p> <p>NHS Code of Practice on Protecting Patient Confidentiality (2012)</p> <p>NHSScotland records management code of practice (v2.1, 2012)</p> <p>External docs</p> <p>Disposal and Destruction of Sensitive Data (HSCIC 2015)</p> <p>HMG IA5 Secure Sanitation (UNCLASSIFIED) (Cabinet Office, v4 April 2011)</p> <p>Disposal and Destruction of Sensitive Data (HSCIC 2015)</p> <p>CPNI Multi Function Device (MFD) security guide (CPNI 2011)</p> |
|  | <h2>Access control</h2> <p>NHS Scotland docs</p> <p>Accessing Personal Information on Patients and Staff: A Framework for NHS Scotland Access Protocol template (March 2010)</p> |

| | |
|---|---|
| | <p> Access Protocol Guidance Note (March 2010) SWAN Information Security Policy (v1.0 PDF) (2015) SWAN Tier 1 Code of Connection (v1.0 PDF) (2015) SWAN Tier 2 Connect Agreement (v1.0 PDF) (2015) Handling Requests For Access To Personal Health Data (November 2011) Accessing personal information of patients and staff – framework NHSScotland Authentication Good practice guide (May 2012) </p> <p>External docs</p> |
|  | <h2>Cryptography</h2> <p>NHS Scotland docs</p> <p>External docs</p> <p>Approved Cryptographic Algorithms (HSCIC v3.0 2012)</p> |
|  | <h2>Physical and environmental security</h2> <p>NHS Scotland docs</p> <p>SWAN Information Security Policy (2015)</p> <p>External docs</p> <p> Physical security over IT (CPNI 2014) protection of data centres (CPNI (2012) Security doorsets and locking hardware (CPNI 2012) </p> |
|  | <h2>Operations security</h2> <p>NHS Scotland docs</p> <p> NHS D&G Internet Use and Monitoring Policy (example, v2.0 Jan 2008) Managing Information Assurance for Mobile Wireless Services in NHS Scotland </p> |

| | |
|---|--|
| | <p>External docs</p> <p>Anti-virus and Malware GPG (HSCIC v2.0 2010) GPG13 – Protective Monitoring (CESG Oct 2012) Good Practice Guide for Computer-Based Electronic Evidence (ACPOS) Patch Management (HSCIC v1.0 Oct 2009) System Hardening (HSCIC v1.0 Sep 2009)</p> |
|  | <p>Communications security</p> <p>NHS Scotland docs</p> <p>Application – Web Service Security Standard Using eMail in Scotland: A Good Practice Guide 2014 Frequently Asked Questions on New Guidance for eMail in NHSScotland SMS Good Practice Guide (August 2012) Intra NHS Information Sharing Accord</p> <p>HSCIC docs</p> <p>Access Control List GPG (HSCIC v2.0 Feb 2009) Application Security (HSCIC 2007) Firewall Technologies (HSCIC v1.0 Dec 2007) Local Area Network Security (HSCIC v2.0 Sep 2009) Securing Web Infrastructure and supporting services (HSCIC v1.0 Feb 2010) Intrusion Detection and Prevention Systems(IDS/IPS) (HSCIC v2.0 Sep 2009) Virtual Local Area Networks (VLANs) (HSCIC v2.0 Mar 2009) TCP/IP Ports and Protocols (HSCIC v1.0 Aug 2007) Network Address Translation (NAT) (HSCIC v2.0 Jan 2010) Site to Site VPN (HSCIC 2006)</p> <p>Other external docs</p> <p>Web services – hacking and hardening (OWASP, Layer 7, 2007) Architectural Pattern 12 – Wireless Networking (CESG, Version 1.0, Feb 2013) SP800-97 (Establishing Wireless Robust Security Networks) (NIST, Feb 2007) sp800-41-rev1 (guidelines on firewalls and firewall policy) (NIST 2009) SP800-44v2 (securing public facing servers) NIST (2007)</p> |

| | |
|---|---|
|  | <p>System acquisition, development and maintenance</p> <p>NHS Scotland docs</p> <p>External docs</p> <p>General Principles for Securing Information Systems (HSCIC v1.0 May 2009)</p> |
|  | <p>Supplier relationships</p> <p>NHS Scotland docs</p> <p>CEL2011_25 (Safeguarding confidentiality in third party agreements) (2011)</p> <p>External docs</p> <p>UK Government Legal Services – Model Services Contract</p> <p>Security in the supply chain (CPNI 2015)</p> <p>Security governance framework for IT managed services (CPNI 2009)</p> |
|  | <p>Information security incident management</p> <p>NHS Scotland docs</p> <p>Significant Incident Reporting Guidance (2014)</p> <p>External docs</p> |
|  | <p>Information security aspects of business continuity management</p> <p>NHS Scotland docs</p> <p>External docs</p> |

| | |
|---|--|
| | <p>Business Continuity and Disaster Planning GPG (HSCIC v1.0 Sep 2009)</p> |
|  | <p>Compliance</p> <p>NHS Scotland docs</p> <p>NHS Factsheet on Protecting Patient Confidentiality</p> <p>External docs</p> |
|  | <p>Additional categories</p> <p>Technical standards</p> <p>Infrastructure Standard v1.1 Video Conferencing Standard v1.0 Application – User Interface Standard Server Virtualisation Security (HSCIC v1.0 July 2009)</p> <p>Use of social media</p> <p>NHS Scotland Online Document Sharing GPG (SG eHealth 2013) Harnessing Online Social Networking within NHSScotland: Benefits and Risks (October 2011) Policy and Good Practice Guidelines for the Use of Social Media (NHS NES, v1.0 Sep 2010) Virtualisation</p> <p>NHS focussed standards</p> <p>Clinical Document Indexing Standard v2.8 (Sep 2015) Clinical Information Presentation Standard V5.2 International Classification of Diseases (ICD) 10 Edition 4 – Standard The use of the CHI (Community Health Index) across NHS Scotland (June 2013) Extension of Emergency Care Summary (ECS) Access to Scheduled Care Settings in Support of Medicines Reconciliation</p> |

| | |
|---------------------------|--|
| Document control | |
| Version | 4.1 Final version approved by Staff Governance Committee |
| Title | NES Information Security Policy |
| Summary | A policy document detailing the management and reporting structure for Information Security. |
| Date | November 2016 |
| Author | Information Governance Manager (Frank Rankin) |
| Owner | Senior Information Risk Owner, Christopher Wroath |
| Document No. | IGP004 v 4.1 |
| Document location: | Alfresco Digital Site |

| Authorisation | | | |
|-------------------------|----------------------------|---|----------------|
| Approved by | Staff Governance Committee | | |
| Date of approval | 10 November 2016 | | |
| Date of Issue | 21 November 2016 | | |
| Supersedes | IGP004 v 3.3 2011 | | |
| Date for review: | November 2018 | | |
| Version history | | | |
| Date | Version | Status/ Summary of changes | Author |
| March 2011 | 3.0 | Initial draft for consideration by IG Group | Frank Rankin |
| May 2011 | 3.1 | Redrafted to accommodate comments of IG Group and ISO consultant. As presented for consultation | Frank Rankin |
| May 2011 | 3.2 | Amendment to p. 5 re corporate systems | Deborah Dillon |
| July 2011 | 3.3 | Incorporating comments from F Torrens As presented to Partnership Forum | Frank Rankin |
| August 2013 | 3.4 | Reviewed and updated for submission to IGG | Frank Rankin |
| February 2014 | 3.5 | Amended in line with IGG Comments, UK classification revision and BYOD | Frank Rankin |

| Authorisation | | | |
|----------------|------|--|--------------|
| February 2014 | 3.6 | As approved by Digital Engagement Group and sent for consultation and EQIA. | Frank Rankin |
| August 2014 | 3.7 | Incorporates comments from staff side. | Frank Rankin |
| October 2014 | 3.8 | Following staff consultation | Frank Rankin |
| June 2015 | 3.9 | Amended to accommodate changeover from ISO27001:2005 to ISO27001:2013 and management changes to Digital Directorate. | Nick Cowan |
| August 2015 | 3.10 | Amended to accommodate ISO27001:2013 requirements and include reference to NHS Scotland Info Sec framework. Added to NES Digital document template | Frank Rankin |
| September 2015 | 3.11 | Reorganised to transfer relevant content to separate End User Info Sec Policy | Frank Rankin |
| January 2016 | 3.12 | Revised to include content from NHS Scotland Info Sec policy | Frank Rankin |
| February 2016 | 3.13 | Revised to include points from Secure Development meeting | Frank Rankin |
| July 2016 | 3.14 | Amended draft for consultation, incorporating SIRO comments | Frank Rankin |
| October 2016 | 4.0 | Revised to include new Top Management Group. Version for submission to Partnership Forum and Staff Governance Committee | Frank Rankin |



NHS Education for Scotland
Westport 102
West Port
Edinburgh EH3 9DN
tel: 0131 656 3200
fax: 0131 656 3201