Information Security

1.04 Asset Management All User Standard

Approval

Document Reference	Information Security – 1.04 Asset Management – All User Standard
Version	0.3
Last updated	1st March 2021
Owner	
Approval by	

Contents

1. INTRODUCTION

Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) (herein HSC will refer to all HSC and NIFRS organisations) Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

This standard sets out the principles and security requirements for the introduction, use, decommissioning, redeployment and disposal of hardware and software assets. Examples of Information Assets include any HSC information that has value including but not limited to, hard and soft copy computer data, customer information, personal information, intellectual property, business sensitive information and information used for a business process.

Examples of Information Systems covered by this standard include, but is not limited to, devices that process and analyse HSC Information such as network devices, computers, mobile devices and software programs, and HSC business procedures. This standard will support consistency, adherence to common standards and sustainability with regard to asset management across HSC organisations.

2. PURPOSE

This Information Security Standard is in place to ensure HSC and NIFRS organisations are able to manage Information Assets and Systems in a manner that is effective for the business need, whilst reducing the risk of any losses related to the Confidentiality, Availability or Integrity of HSC and NIFRS Information Assets and Systems.

2.1.1. For more information, Technical users should see:

- Information Security 2.01 Asset Management Standard;
- Information Security 2.10 Network Discovery Standard; and
- Information Security 2.13 Wireless Standard.

3. SCOPE

The Information Security Standard applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS [1], including:
  - HSC and NIFRS employees;
  - Temporary Staff including agency and students;
  - Voluntary Health Sector organisations / Volunteers;

[1] Northern Ireland Health & Social Care organisations include Health & Social Care Board (HSCB), Public Health Agency (PHA), Health & Social Care Trusts, NI Ambulance Service (NIAS), Business Services Organisation (BSO), Patient & Client Council (PCC), Regulation & Quality Improvement Authority (RQIA), NI Guardian Ad Litem Agency (NIGALA), NI Blood Transfusion Service (NIBTS), NI Social Care Council (NISCC), NI Practice and Education Council for Nursing and Midwifery (NIPEC), NI Medical and Dental Training Agency (NIMDTA), GP Practices and other Independent Contractors to HSC, and Northern Ireland Fire and Rescue Service (NIFRS).

    - Third Party Contractors;
    - Any other party making use of HSC ICT resources;
- HSC information stored, or in use, on HSC or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving HSC networks; and
- ICT Systems belonging to or under the control of HSC.

This Standard applies throughout the entire information lifecycle from acquisition/creation through utilisation to storage and disposal.

4. STANDARD NON-COMPLIANCE / BREACH

See the Information Security Policy for details of what to do in the event of non-compliance or a breach of an Information Security Standard. For an information Security Breach or Incident, see the Information Security Incident Identification and Reporting All User Standard.

5. ASSET MANAGEMENT

5.1. INVENTORY OF ASSETS

5.1.1. The ICT department must identify and record all authorised hardware and software in an asset management register.

5.1.2. All external information systems (i.e. third-party information systems that process HSC data and that are not managed by the HSC ICT department) that regularly process HSC data (i.e. subject to a Data Sharing Agreement or who have a processor relationship with HSC) must be recorded in the same manner as if it were a HSC information System, with the clear distinction that it is externally managed.

5.1.3. Asset inventories shall be: backed up, protected from unauthorised access, accurate, up-to-date, consistent and aligned with other inventories.

5.1.4. Asset owners are responsible for ensuring that the asset register is maintained for all assets under their control.

5.1.5. In order to effectively manage assets throughout their lifecycle, assets must be uniquely identified, and the register must contain sufficient information. The asset register should include the following information as a minimum:

- Asset Owner/s;
- Asset Classification/s (e.g. business criticality, information classification or information security impact rating);
- Asset type;
- Associated systems;
- Current deployment history;

- Version of the asset;
- Format;
- Asset's purpose;
- Location (to include data flow – storage, transmission and processing);
- Backup information; and
- License information.

5.1.6. The asset register must be reviewed annually and updated upon major changes. This, in addition to each organisation's compliance requirements for licensing, enables the business to:

- Identify discrepancies or gaps in the register;
- Detect any use of software that is unlicensed or has expired; and
- Show potential areas of fraud, theft or misuse of equipment.

5.1.7. Tools must be used to identify unauthorised hardware or software.

5.2. OWNERSHIP

5.2.1. HSC assets associated with information and information processing must have an assigned owner. Ownership ensures who is responsible for the confidentiality, integrity and availability of that asset.

5.2.2. A process to ensure timely assignment of asset ownership must be implemented, (e.g. ownership must be assigned when the assets are created).

5.2.3. The asset owner must be responsible for the management of an asset over the entire lifecycle of the asset.

5.2.4. An asset owner must be allocated to a role that is accountable for the asset during its lifecycle. Asset ownership can be different to legal ownership and it can be done at an individual, department, or organisational level.

5.2.5. The asset inventory must be updated upon a change of ownership.

5.3. ACQUISITION OF ASSETS

5.3.1. Acquisition of assets not on the approved asset register must be managed in accordance with an HSC asset selection and approval process.

5.4. ASSET SELECTION AND APPROVAL

5.4.1. Prior to use, new asset types must be reviewed and approved by IT to ensure security risks associated with use of the asset are identified and managed.

5.4.2. All assets must be procured according to local procurement policies and processes.

5.5. PROTECTION OF ASSETS

End Users

5.5.1. All staff shall ensure they take reasonable precautions to protect HSC information assets and systems, including but not limited to:

- Not leaving assets unattended;
- Making use of privacy screens;
- Not allowing individuals to see or hear information that they are not authorised for; and
- Keeping personal authentication information, i.e. keeping passwords secure.

5.5.2. Regular training and compliance activities must be undertaken by staff to ensure they understand the risks to HSC Information assets and systems and that they are enabled to provide adequate protection.

5.5.3. Information classification of HSC data is mandatory to ensure that ICT managed assets are adequately and proportionately protected. The level of classification determines the type of information that is allowed to be stored on specific assets and is determined according to local policy by the Information Asset Owner.

5.5.4. Staff must report all lost assets to Line Managers and the local ICT department immediately and if applicable a DATIX incident must be raised

System Owners

5.5.5. An appropriate set of procedures for information labelling must be developed and implemented in accordance with the Local Information Classification Policy adopted by the organisation. Procedures for information labelling must cover information and related assets in both physical and electronic formats.

5.5.6. Controls in place to protect assets must be commensurate with the classification of the information stored on, processed or transmitted by the asset. Refer to the Local organisation's Information Classification Policy for more detail.

5.5.7. Agreements with other organisations that include asset sharing, must include procedures to identify the classification of information associated with these assets and to interpret the classification labels from other organisations.

5.5.8. The local IT department must ensure that all reasonable efforts are taken to find any lost assets and that the loss is reported appropriately. The IT department or Line Manager may be required to inform the Data Protection Officer as defined under the General Data Protection Regulations (GDPR). A DATIX incident should be completed if required.

5.6. ASSET HANDLING

5.6.1. Procedures for handling assets need to be developed and implemented in accordance with the local information governance policy. This must be done for all

forms of assets regardless of where they are in the asset lifecycle. The following must be considered:

- Access restrictions for each level of classification;
- Maintenance of a formal record of the authorised recipients of assets;
- Storage of IT assets in accordance with manufacturers' specifications;

5.7. STORAGE MEDIA HANDLING

5.7.1. All media must be stored in a safe, secure environment, in accordance with manufacturers' specifications and additional techniques, such as encryption, considered where appropriate.

5.7.2. Authorisation must be obtained prior to removing media from the organisation, and a record must be kept in order to maintain an audit trail.

5.7.3. When no longer required, storage media, or the data it contains, must be disposed of securely by following documented procedures. The procedures must be proportional to the sensitivity of the information being disposed. The contents of any re-usable media shall be made unrecoverable and securely destroyed or erased.

5.8. REDEPLOYMENT, DECOMMISSIONING AND DISPOSAL

End Users

5.8.1. Upon termination of employment, contract or agreement, all issued HSC assets must be returned to the local organisation.

5.8.2. Employees, contractors or third parties who have used a personal device to access HSC information, must agree and comply with the terms and conditions enabling the secure transfer and deletion of the information.

5.8.3. It is the responsibility of the employee, contractor or third party to ensure the preservation of their own personal data (unrelated to HSC controlled personal data) before an asset is wiped for redeployment or disposal.

System Owners

5.8.4. A documented process must exist to ensure that the return of assets is appropriately managed and can be evidenced for each person or third party. Refer to the local Joiners, Movers and Leavers Policy for more information.

5.8.5. Where HSC assets are not returned according to the process, unless otherwise agreed and documented as part of the exit process, a security incident must be logged.

5.8.6. Prior to redeployment, decommissioning, or disposal, all information must be securely erased from the asset. The method of erasure must be appropriate for

the type and sensitivity of the information asset or system. Please refer to the Information Security 1.08 Encryption Standard.

5.8.7. Where the information cannot be deleted (e.g., asset is faulty or has failed), the asset must be securely destroyed.

5.8.8. Assets that are not in use and awaiting deletion or destruction must be securely stored and access restricted to personnel involved in the disposal process.

5.8.9. Redundant assets must be disposed of in accordance with relevant legal, regulatory and contractual obligations.

5.8.10. The asset register must be updated with the new status of the asset upon a change.

5.9. Records Management

5.9.1. A formal documented standard for records management must be developed and embedded within each organisation. Refer to the local information governance policy for more detail.

6. MONITORING

Staff must be aware that any data on the organisation's systems remains the property of HSC. HSC reserves the right to monitor and record any use of organisation information and systems to ensure they are used for legitimate purposes, and that policies and standards are being complied with.

All monitoring must be undertaken in accordance with the appropriate legislation such as Regulation of Investigatory Powers Act (2000), Human Rights Act (1998), and good practice guidance such as "Employment Practices Code Part 3: Monitoring at Work" issued by Information Commissioners Office.

A periodic audit of assets to ensure their continued protection must take place. All users must co-operate fully with any such audit.

A review of asset management will be carried out annually.

7. REVIEW CYCLE

This policy will be subject to annual review or following any significant incidents, changes to legislation or changes to the HSC structure or functional responsibilities.

<<Add Name>>.

<<Add Role>> Date: 25/02/2020

<<Add Name>>.

<<Add Role>> Date: 25/02/2020