NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

HSC Information Security Policy and User Standards

February 2024

Any request for the document in another format or language will be considered

James House
2-4 Cromac Avenue
Belfast
BT7 2JD
Tel: 0300 300 0066

https://nipec.hscni.net

Developed by:	**Business Support Manager**
Approved by / date:	**Business Team: 5 March 2024** **NIPEC Council: 13 March 2024**
Date of next Review:	**October 2027** or following any significant incidents, changes to UK or EU legislation or changes to the HSC structure or functional responsibilities.
Equality Screened by / date:	**Business Support Manager – March 2024**

TABLE OF 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. It is, however, vulnerable to risk and so there is a need to develop a culture within which our Information Assets and Systems can operate efficiently, effectively and securely. The management of these risks is referred to as Information Security which is used herein to describe the management of risks relating to Information Assets and Systems.

HSC takes a risk-based approach to the management of Information Security risk, and objectives outlined in this policy and the supporting Information Security Standards aim to target and treat the highest risks to the organisation. An example of this is malicious or accidental insider threat, which remains a big risk to HSC, so effective Information Security management requires the participation of all NIPEC/HSC employees in the organisation.

Information Security can be achieved in part through technical means but should be supported and enhanced by appropriate management and procedures. The main principle is that the data and information that HSC information systems process (particularly personally identifiable and business sensitive data) must only be seen by those who are entitled to see it.

HSC is committed to the continuous improvement of Information Security across our organisations and commit to satisfy the applicable ethical, regulatory and legal requirements. To enable this, the objectives set out within this Information Security Policy are complemented by the following set of detailed Information Security Standards, for non-technical users.

Standard Reference Number	User (non-technical) Standards
1.01	Email Communications
1.02	Removable Media
1.03	Use of Internet Services
1.04	Asset Management
1.05	Clear Desk and Screen
1.06	Cloud Security
1.07	Data Transfer
1.08	Encryption
1.09	Incident Identification and Reporting
1.10	Remote and Mobile Working
1.11	Accounts and Passwords

Copies of these non-technical User Standards are appended and should be read in conjunction with this document.

There are a number of relevant pieces of legislation that must be adhered to if HSC organisations are to remain legally compliant when using, storing and handling information. The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulations (GDPR) place a legal obligation on UK organisations to take steps to ensure that personal data is adequately protected. HSC is also required to abide by the Network and Information Systems (NIS) Regulation 2018 that aims to improve the cyber security and resilience of key systems.

As the risk to HSC or the regulatory/legal landscape changes, policies and the applicable standards, processes, procedures and guidance will be updated as appropriate.

2 Purpose

This Information Security Policy details the regional approach to Information Security Management across the HSC and NIFRS, including the overall management structure and key principles which apply to each HSC organisation and NIFRS.

This policy, and the associated Information Security standards, lay down high-level principles and expectations, from which each HSC organisation and NIFRS must develop their own local policies, standards, guidelines and working practices to ensure compliance. This policy articulates the NIPEC local policy.

This will ensure a consistent and high standard of Information Security management across the entire HSC and NIFRS community from all significant threats whether internal, external, deliberate or accidental.

3 Scope

This Information Security Policy applies to:

- All parties who have access to, or use of Information Assets and Systems belonging to, or under the control of HSC or NIFRS, including:
    - NIPEC (including Associates) and HSC/NIFRS employees
    - Temporary Staff, including agency workers and students
    - Business Services Organisation IT Services Unit (BSO ITS) Staff, responding to INFRA Requests, and/or who are conducting work on behalf of NIPEC
    - Voluntary Health Sector organisations/Volunteers
    - Third Party Contractors
    - Any other party making use of HSC ICT information resources
- Information stored, or in use, on HSC ICT or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving the HSC networks;
- ICT Systems belonging to or under the control of HSC.

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

4 Management Framework

4.1 Strategic Direction

The Department of Health (DoH) in Northern Ireland is responsible for setting policy and legislation which directs Information Security Management across the HSC.

The Strategic Planning and Performance Group (SPPG) is responsible for the effective commissioning of Information Systems across the HSC estate, the provision of delegated funding to meet agreed objectives in line with ministerial and departmental policy and the implementation of performance management and service improvement to monitor objectives, targets and standards and their achievement.

4.2 Co-ordination

HSC co-ordinates Information Security management across the region through the Cyber Programme Board. This group holds responsibility for considering and proposing amendments to Information Security management. Significant amendments will be approved by the Chief Digital Information Officer and External Collaboration.

HSC co-ordinates Information Governance management across the region through an internal Information Governance Advisory Group, chaired by the Head of Information Management Branch of the DoH.

4.3 Core Infrastructure

The Business Services Organisation IT Services Unit (BSO ITS) provides and maintains the central IT infrastructure and architecture for HSC. This includes providing Technical Design Authority support (which has representatives from across all HSC organisations and is chaired by Assistant Director of CNI) and General Medical Services ICT support to the SPPG.

4.4 Collaboration

All HSC organisations are expected to work together to ensure the successful implementation and development of Information Security across the HSC.

4.5 Operational Management

4.5.1 HSC Cyber Leads Group

Cyber Leads Group governs local implementation of Information Security management across the region through an internal working group of Information Security representatives from HSC organisations, chaired by the Cyber Leads Programme Manager of the Business Services Organisation (BSO). NIPEC is represented on this group by the Head of BSO ITS.

4.5.2 Local Security Management

Each HSC organisation is responsible for implementing a local programme of Information Security management, including the provision of necessary skills, training and resource to ensure adherence to this policy.

Each HSC organisation is accountable to the DoH, through their Executive and Non-Executive management framework, for the application of this policy.

4.6 Roles and Responsibilities

4.6.1 Chief Executive (Most Senior Officer)

The Chief Executive is responsible to the DoH for Information Security within NIPEC, and is responsible for the following:

- Ensuring a nominated officer with sufficient authority is appointed for security related matters and that these are adopted throughout the organisation;
- Ensuring frameworks are in place for information systems are appropriately assessed for security; and
- Ensuring the organisation maintains compliance with HSC Information Security Policy.

4.6.2 Senior Information Risk Owner (SIRO)

Responsible to the Chief Executive within NIPEC, advising on the information risk aspects of his/her statement on internal controls. Within NIPEC, the Head of Corporate Services fulfils this role, and is responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation;

- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners; and
- Owning the organisation's information management process.

4.6.3 Data Protection Officer (DPO)

Reporting to the SIRO, the DPO is an independent Data Protection expert who is accountable for ensuring Data Protection regulations such as the DPA and UK GDPR are being successfully managed by the organisation. NIPEC's DPO function is provided via an annual Service Level Agreement with BSO.

The DPO is responsible for:

- Informing and advising HSC data protection obligations, monitoring internal compliance, and demonstrating compliance where required;
- Providing support and advice tp the organisation on Data Protection matters generally and also the Data Protection Impact Assessment (DPIA) process; and
- Being the point of contact for data subjects and the supervisory authority (Information Commissioner's Office [ICO]).

4.6.4 Information Asset Owners (IAO)

Responsible to the SIRO within NIPEC providing assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Within NIPEC, Senior Professional Officers, the Senior Communications Manager and Business Manager fulfil these roles, and are responsible for the following:

Responsible for:

- Knowing what information comprises or is associated with an asset, and understands the nature and justification of information flows to and from the asset;
- Knowing who has access to the asset, why they have access, ensuring access is compliant with all appropriate policies, procedures or standards; and
- Understanding and addressing risks to the asset, and providing assurance to the SIRO.

4.6.5 HSC ICT Security Manager

BSO Information Technology Services (ITS) is the Centre of expertise with responsibility for the operational delivery and support of regional Information and Communications Technology (ICT) Systems to the HSC sector throughout Northern Ireland. This service is provided via an annual Service Level Agreement and includes a Cyber Security Service and management of a Cyber Security Programme to implement regional solutions to improve the effectiveness of cyber security controls in countering cyber-attacks from internal and external threats and assist with ISO27001 accreditation.

The BSO ITS Security Manager is responsible for:

- Co-ordinating Information Security matters across organisational and system boundaries within the HSC;
- Monitoring the effectiveness of Information Security Policy, procedures, standards, guidelines across the HSC;
- Taking a pro-active role in establishing and implementing an HSC-wide Information Security Programme including training, awareness and guidance;
- Promoting Information Security awareness across the HSC;
- Receiving and considering reports of Information Security incidents from the ICT Security Managers/Officers, Systems Managers or others, ensuring the necessary corrective or preventative actions are implemented; and
- Liaising with ICT Security Managers/Officers on matters of Information Security which may impact multiple HSC organisations.

4.6.6 Cyber Lead

This service is provided via an annual ICT Service Level Agreement which includes a Cyber Security Service and management of a Cyber Security Programme to implement regional solutions to improve the effectiveness of cyber security controls in countering cyber-attacks from internal and external threats and assist with ISO27001 accreditation.

4.6.7 System Managers/Information Asset Administrators (IAA)

Responsible to the Information Asset Owners (IAO) within NIPEC, ensuring that information security requirements, expectations and limitations are mutually understood and agreed, and processes are in place to securely and effectively manage the day to day operations of HSC information systems.

Responsible for:

- Day to day operational management of the information system including implementation of suitable measures to ensure system is secure;
- Working in conjunction with BSO ITS to ensure core local processes are consistently applied across all information systems;
- Ensuring users of the system are appropriately trained; and
- Reporting security matters to one of the NIPEC IAOs/BSO ITS.

4.6.8 Third Party Contractors:

Responsible to the IAO/Business or Contract Owner/Manager ensuring compliance to regional and local Information Security Policies.

Responsible for complying with the terms of their Statement of Compliance.

4.6.9 Users of Information Assets and Systems

All NIPEC users are responsible for:

- Complying with all NIPEC and regional Information Security policies, procedures or standards;
- Ensuring attendance at, or completion of, all necessary Information Security awareness/training sessions; and
- Reporting adverse incidents relating to Information Security in accordance with local policies, procedures or standards.

5 Policy Statement

5.1 Controls Assurance

All HSC organisations are required to achieve and maintain compliance with the NIS 2018 cyber assessment, and where necessary report to the Competent Authority, in order to provide routine assurance that Information Security is being effectively managed.

To support and underpin compliance all HSC organisations shall have:

- Staff who are well trained to exercise good judgment, take responsibility and be accountable for the information they handle, including all partner information;

- Mechanisms and processes to ensure assets are properly classified and appropriately protected; and
- Confidence that security controls are effective and that systems and services can protect the information they carry.

5.2 Terms and Conditions of Employment

NIPEC will ensure that all contracts of employment include statements requiring compliance with HSC and local Information Security policies & procedures. HSC organisations must ensure:

- Contractual obligations are made clear and employees sign terms and conditions;
- Employees are made aware of their responsibilities and liabilities;
- All employees receive security awareness, education and training;
- A formal disciplinary process for security breaches is in place;
- Employees exit the organisation in an orderly manner;
- Termination or change of employment is clearly defined;
- There are processes for changing or terminating employment and access rights are terminated at the end of employment.

5.3 Third Party Management

HSC organisations must develop and implement a third-party risk management framework to ensure that strategic, business and budget objectives have rigour, and the selections of products and supplier services are based on an organisational acceptance and understanding of risk.

All HSC organisations must ensure that Information Security clauses, particularly with regards to the DPA 2018, NIS 2018 and UK GDPR, are built into all formal service contracts where required.

Where third parties have access to HSC networks, HSC organisations must document the standards and processes necessary to protect against supply chain threats to connected information systems, system components, or information system services. An adequate and proportionate monitoring and auditing capability is expected commensurate with Information Security based risks.

Where data is being hosted externally to the HSC networks (e.g. Cloud Services), information-based risk assessments must be carried out in line with the Information Security Technical Standards. These assessments must, as a minimum, consider legislation and implications with regards to:

- Processing of Personal Data;
- Hosting outside the EU (if applicable);
- Business continuity planning;
- Physical and logical access management;
- Information protection (at rest and in transit);
- Disposal of information;
- Audit logging and access to logs/reports; and
- Termination of contract.

5.4 Data Classification

All HSC organisations must ensure that information assets and systems are classified appropriately, taking into account value, relevant legal requirements, sensitivity and criticality to the organisation.

The NHS Digital Risk Model should be used to help inform HSC organisations ensure an appropriate and consistent set of processes and procedures are developed, including:

- Defining information;
- Classifying information;
- Accepting ownership for classified information;
- Labelling classified information;
- Storing and handling classified information;
- Managing network security;
- Categorising and labelling Personally Identifiable Information according to its
- sensitivity; and
- Making distinctions between ordinary personal data and special categories of personal data as required.

5.5 Records Management

All HSC organisations must ensure that standards and processes are in place and compliant with the Department of Health “Good Management, Good Records” guidance to appropriately document, maintain and destroy HSC information throughout its lifecycle.

The integrity of HSC information relies on information being trusted, acceptable, useable and available. Information should be in a format that is accessible and easy to use, whether it is in electronic, photographic or paper form whilst being adequately protected from unauthorised modification or access.

5.6 Encryption

All HSC organisations must document the standards and processes necessary to ensure personally identifiable or business sensitive information which is held on devices (including laptops, mobile devices and removable media) and transmitted via the internet, is encrypted to the HSC approved standards, as mandated by the DoH.

All HSC organisations must ensure that standards and processes are in place to outline the appropriate requirements for protecting encryption keys against compromise, damage, loss and unauthorised access.

Further guidance is provided in the Information Security Encryption Standard (Appendix 8).

5.7 Information Asset and System Management

All HSC organisations must ensure that standards and processes are in place for the secure recording, monitoring, use, maintenance, decommissioning, redeployment and disposal of all information assets (including hardware and software).

All HSC organisations must ensure that standards and processes are in place to maintain software integrity and traceability. These should govern:

- Procurement of software;
- Risk management;
- The software installation process (and licensing requirements);
- Network management (where software utilises the network);
- Set standards and processes for updating software; and
- The end-of-life process for software (including the removal of software/ licensing, and deletion/transfer of associated data).

Further guidance is provided in the Information Security Asset Management Standard (Appendix 4).

5.8 Data Protection

The legal requirement for the lawful and correct handling of personal data is set out in the DPA 2018. This Act makes provision for the regulation of the processing (collection, handling and storing etc.) of information relating to living individuals, including the obtaining, holding, use or disclosure of such information. HSC Organisations must have local a Data Protection Policy(s) to ensure the DPA 2018 requirements are met.

All HSC organisations must ensure standards and processes are in place to facilitate implementation of the local Data Protection policies and associated system/information integrity controls. These must include requirements on how personal data must be processed to meet the HSC's data protection standards and to comply with the law, see local policy for more information.

The Code of Practice on Protecting the Confidentiality of Service User Information document issued by DoH in April 2019 provides guidance on the handling of personal information and should be applied by HSC organisations.

HSC organisations must ensure that safeguards are in place for information assets and systems, especially those being removed from site for repair or replacement – for example, HSC data or licensed software must be removed prior to disposal or reuse of an asset or system.

5.9 Email Communications

All HSC organisations must ensure that standards and processes are in place to manage email communications that use HSC organisation-controlled email services.

Personal use (any access which is unrelated to official duties) of HSC email services is only permitted in accordance with local security policies – however it shall be avoided where possible.

Further guidance is provided in the Email Communications Standard (Appendix 1).

5.10 Use of Internet Services

All HSC organisations must ensure that standards and processes are in place to manage the use of internet services.

All staff must use internet services in a secure, ethical and legal manner. Staff shall only use internet services for reasonable personal use. Examples of prohibited Internet Services include but are not limited to:

- Attempts to gain unauthorised access to information resources;
- Accessing material that is pornographic, illegal, offensive, or discriminatory;
- Accessing non-approved file sharing services or software;
- Activities that could be damaging to the reputation of the organisation;
- Activities that interfere with business requirements; and
- Activities that violate copyright, license agreements or other contracts.

Further guidance is provided in the Use of Internet Services Standard (Appendix 3).

5.11 Information Flow Control

All HSC organisations must ensure that standards and processes are in place to record, manage, regulate and control the flow of information within HSC systems and between HSC's interconnected systems.

To comply with the UK GDPR and DPA 2018, HSC organisations need to map information flows in order to appropriately assess privacy risks where applicable.

5.12 Data Transfer

All HSC organisations must ensure the parameters for secure and appropriate data transfers are set out. The Information Security content of any Data Access Agreement (DSA) should reflect the sensitivity of the business information involved.

Where formal service contracts are either absent or do not adequately cover the sharing of business sensitive or personally identifiable information between HSC organisations and/or outside organisations, the HSC Data Access Agreement procedure must be followed.

Before establishing any new form of data transfer process that involves personal data, a DPIA must be conducted as a requirement under the DPA 2018/UK GDPR.

Further guidance is provided in the Use of Data Transfer Standard (Appendix 7).

5.13 Accounts and Passwords

All HSC organisations must ensure that standards and processes are in place to ensure access to systems, information and information processing facilities is limited to those with appropriate authority. These should be used to ensure

correct user account provisioning, maintaining appropriate separation of duties between users and outline password best practices.

All HSC organisations must ensure that information systems use unique identifiers for information systems, users and the devices used to access information.

Security privileges and access rights must be allocated based on the requirements of a user's role, and use the principle of least privilege.

Processes must be in place and actioned as soon as is possible to in the event that a user joins the organisation, moves departments (including changing role, or requires different privileges) or leaves the employment of the organisation.

Strong authentication mechanisms must be in place to ensure authorised access.

All staff are responsible for setting passwords that meet the minimum requirements and not sharing their password with others.

Further guidance is provided in the Accounts and Passwords Standard (Appendix 11).

5.14 Acceptable Use

All HSC organisations must ensure that standards and processes are in place to establish the acceptable use of computing equipment and facilities provided by HSC, both from the workplace and whilst using resources remotely. These must be consistent with overarching policies and legislation governing personally identifiable or business sensitive information.

5.15 Remote and Mobile Working

All HSC organisations must ensure that standards and processes are in place to establish secure connections to HSC networks or systems from any remote host using Multifactor Authentication (MFA) where possible.

Restrictions and configuration requirements for organisation-controlled devices should be established to minimise their potential exposure to compromise, which may result from unauthorised use of HSC resources.

All staff are responsible for the authorised and appropriate use of all remote resources, complying with HSC policies, standards, procedures, and legal responsibilities. Remote resources include, but are not limited to, laptops, smartphones, tablets, workstations, mobile devices, network resources, software and hardware.

Staff must ensure they safeguard remote devices from theft, loss or unauthorised access.

Further guidance is provided in the Remote and Mobile Working Standard (Appendix 10).

5.16 Malware and Endpoint Protection

All HSC organisations must ensure that standards and processes are in place to establish requirements for the detection, prevention and recovery controls to protect against malware - the implementation (software, deployment, update schedule, proactive scanning etc.) and user awareness strategies should also be included (BSO ITS SLA)

Additional controls such as prohibiting unauthorised software install, malicious website deny lists, vulnerability/patch management, business continuity planning etc. should be considered to reduce the risk and impact of malware.

5.17 External Gateways

All HSC organisations must ensure that standards and processes are in place to ensure that external gateways to HSC networks are:

- Notified to the Regional Director of eHealth and External Collaboration;
- Controlled by a suitably configured firewall that is at least Common Criteria EAL4 compliant;
- As a minimum, when new services are brought online, or when significant changes are made, the use of the CHECK scheme is recommended;
- Subject to annual health checks; and
- Remediated in line with agreed risk appetite and local policy where a vulnerability has been identified.

Where external gateways facilitate internet access, a suitable monitoring solution must be in place.

Consideration should also be given to installing Intrusion Prevention and SSL inspection systems on external gateways.

HSC shall consider additional security controls at connection points to the HSC network such as firewalls. This is especially important if inbound initiated connections are permitted at the external gateways, to give security assurance to the other HSC organisations on the HSC network.

5.18 Security Training and Awareness

All HSC organisations must ensure that standards and processes are in place to ensure employees and contractors are aware and educated on their responsibilities for Information Security.

Security training and awareness should take place at least annually and be tailored to Information Security risks, taking into consideration the employees' roles and access within the organisation.

The awareness programme should be updated regularly so it stays in line with current risks faced by HSC, organisational policies and procedures and should be built on lessons learnt from Information Security incidents.

5.19 Cloud Security

All HSC organisations must ensure that standards and process are in place to support the secure implementation, risk management and use of cloud services. Use of cloud services within NIPEC must be agreed with BSO IT Service and approved by the SIRO (Head of Corporate Services).

Further guidance is provided in the Cloud Security Standard (Appendix 6).

5.20 Business Continuity

All HSC organisations must ensure that they develop and maintain business continuity and disaster recovery plans, based on business impact and risk assessments, to maintain adequate levels of HSC services in the event of any significant disruption to facilities or information services. These processes should be developed, tested and maintained in conjunction with data owners to ensure they are sufficient to provide an adequate level of service and recovery time.

5.21 Incident Idenitification, Management and Reporting

All HSC organisations must ensure that standards and processes are in place to establish a consistent and effective approach to Information Security incidents, including identification, management and reporting. These are important in complying with legal and regulatory responsibilities, protecting the reputation of HSC organisations and protecting client confidentiality.

All Information Security Incidents or significant threats which may impact other HSC organisations should be shared promptly via agreed processes to assist in incident preparedness, response and recovery processes as appropriate.

All HSC organisations should provide incident statistics to the BSO ITS Cyber Programme Manager, in order to share learning and inform discussions regarding operational matters.

All staff shall report suspected or confirmed incidents to their local ICT service desk immediately.

Further guidance is provided in the Information Security Incident Identification and Reporting Standard (Appendix 9).

5.22 Data Backup

All HSC organisations must ensure that standards and processes are in place to ensure backup copies of information are made and tested regularly. The requirement to backup will be determined based upon, but not limited to:

What the information is, for example:

- User storage;
    - File repositories;
    - Software files;
- The risk to the information;
- Laws and regulations;
- Security controls;
- Information governance requirements;
    - Retention period;
    - Classification and handling procedures.

5.23 Removable Media Handling

All HSC organisations must ensure that standards and processes are in place to govern the secure use, handling and destruction of removable media.

All staff should be aware that:

- Only organisation approved, and encrypted, removable media devices shall be used to store, download or transport organisation and client information;
- Unknown removable media must not be connected to an HSC computer system (e.g. a USB Flash Drive found internally or externally to HSC
- premises) but should, instead, be handed to the ICT Service Desk.

Further guidance is provided in the Removable Media Standard (Appendix 2).

5.24 Security Vetting

All HSC organisations must ensure that standards and processes are in place to screen individuals prior to authorising access to information systems and to rescreen individuals according to defined conditions.

5.25 Physical and Environmental Security

All HSC organisations must ensure that standards and processes are in place to implement and monitor physical security controls to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

The physical security and controls must be actioned in line with the Risk Management Policy, e.g. controls must be relative to the value and potential risk to Information Assets and Systems within those physical boundaries. As a minimum, the policy should set out access authorisations and controls, verification, ingress and egress.

Best practice (such as HMG Civil Contingencies Act 2004 guidance) on monitoring and emergency planning should be included within the policy.

Health and Safety legislation must be adhered to at all times and realised in local policies, standards, processes and guidance materials where applicable. locked areas, desks, printers, cupboards, desk drawers, multi-function devices and photocopiers and computer equipment.

5.26 Clear Desk and Screen

All HSC organisations must ensure that standards and processes are in place to establish the minimum requirements for a clear desk and screen environment. The policy must address security guidance on both the physical environment (e.g. HSC recognises the importance of protecting information), therefore all staff must:

- Collect printed media immediately from printers, especially when printing sensitive information;
- Keep desk areas clear;
- Remove materials from meeting rooms;
- Dispose of any confidential materials in a secure manner;

- Lock sensitive documents in approved drawers and lockers when not in use and keep keys in a secure location;
- Secure PCs, laptops etc before leaving them unattended by locking the screen, logging off or shutting down;
- Ensure on-screen or desk content cannot be overseen by unauthorised individuals, especially when in public places (e.g. use display screen protectors).

Further guidance is provided in the Clear Desk and Screen Standard Appendix 5).

5.27 Risk Analysis & Management

HSC organisations must ensure that standards and processes are in place to ensure the identification, assessment and management of Information Security risks to HSC information assets and systems in accordance with the HSC Risk Management Policy.

5.28 Audit and Accountability

All HSC organisations must ensure that standards and processes are in place to provide auditable evidence for system transactions and that key records are available for a sufficient amount of time (as determined and justified by the Information Asset Owner in line with legal requirements, such as Data Retention).

Audit records, review, analysis and reporting shall be protected from unauthorised access, modification and deletion.

6 Compliance (Legal / Contractual)

In the event of any ambiguity or contradiction in Information Security Policy/Standard material, the more restrictive control statement should take precedence, unless there is an approved business requirement at the local organisation.

To enable HSC organisations the ability to make local decisions balancing both risk and benefit, along with legislative baseline contractual terms and obligations, this Information Security Policy sets out minimum expectations. The accompanying Information Security standards provide more detailed expectations but allow for a greater degree of local decision making by limiting mandates and allowing for local risk assessment, interpretation or judgement where possible.

Exceptions may be permitted through local approval processes. Refer to the policy or standard owner for further guidance or clarification.

7 Reporting of an Information Security Incident

Information Security incidents must be identified and subsequently reported to the BSO IT service desk, or other local incident reporting process, as soon as is possible:

- When a security control has been breached;
- In case of a failure of a security measure that potentially or actually has a detrimental effect to the confidentiality, integrity and/or availability of HSC information assets or systems;
- When unusual behaviour is detected through protective monitoring;
- Where actual or suspected loss/theft of HSC hardware has occurred;
- Non-compliance with policies and guidelines

Further guidance is provided in the Incident Identification and Reporting Standard (Appendix 9).

8 Non-Compliance / Policy Breaches

Sanctions

8.1 Failure of HSC Organisations

Where an HSC organisation is found to be in breach of this policy it is expected that that HSC organisation will investigate in accordance with The Regional Incident Management Process and report their findings to the BSO ICT management framework group.

If the breach is deemed significant enough to put other HSC organisations at risk, it may be necessary to limit or remove access to regional IT health systems and/or other HSC organisations. Any eventual end action required will be taken by the Chief Digital and Information Officer, DoH.

Where serious breaches have occurred, it may also be necessary to report to the Information Commissioners Office for a Personal Data Breach (DPA 2018, GDPR 2018), the Competent Authority where required for a NIS Regulation (NIS 2018) incident, or other appropriate regulatory bodies.

8.2 Failure of HSC Employees

Where an HSC employee is found to be in breach of this policy it is expected that the employing HSC organisation will investigate in accordance with Adverse/Serious Adverse Incident procedures, which may result in the initiation

of disciplinary action and/or initiation of criminal/civil proceedings. Where serious breaches have occurred, it may also be necessary to report to the Information Commissioners Office or other appropriate regulatory bodies.

8.3 Failure of third parties, temporary/agency staff, students or any other party making use of HSC Informaiton Assets and Systems

Where an individual is found to be in breach of this policy it is expected that the employing HSC organisation will investigate in accordance with Adverse/Serious Adverse Incident procedures, which may result in the termination of the contract and/or initiation of criminal/civil proceedings. Where serious breaches have occurred, it may also be necessary to report to the Information Commissioners Office or other appropriate regulatory bodies.

9 Monitoring

Staff should be aware that any data on the organisation's systems remains the property of HSC. HSC reserves the right to monitor and record the use of any organisational information and systems in order to ensure that they are being used for legitimate purposes and that relevant 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.

10 Related Policies, Procedures and Legislation

All HSC organisations should ensure that, as a minimum, they have local policies, standards, procedures, and guidelines, to meet the requirements of the HSC Information Security Policy and associated All User Standards as listed in the Appendices of this policy.

Legislation imposes a need for all HSC organisations to take steps to ensure compliance with all statutory requirements. A list of Information Security frameworks, legislation, regulation and guidance have been used to underpin the development of this policy - note this list is not exhaustive – and can be found in Appendix 11.

APPENDIX 1

1.01 Email Communications All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

The HSC email system is a significant business, information and communication tool, yet email also poses a significant risk to Information Security. The sensitive nature of the communications sent via email and the high usage of email, mixed with the high likelihood of error and malicious use of email mean that data breaches are likely and could result in harm to individuals, and subsequent regulatory actions being taken against HSC.

PURPOSE

This Information Security Standard is in place to ensure HSC organisations are able to use their email services 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 or NIFRS Information Assets and Systems.

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, including:
    - HSC and NIFRS employees
    - Temporary Staff including agency and students
    - Voluntary Health Sector organisations / Volunteers
    - 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;
- 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.

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.

EMAIL COMMUNICATIONS

Email Usage

All staff shall exercise good judgement and use the email system in an acceptable manner and in accordance with all relevant Policies and Standards. Examples of prohibited uses include but are not limited to:

- Transmitting confidential or organisation information to unauthorised individuals;
- Transmitting material that is illegal, offensive or discriminatory;
- Transmitting any material or communication that could be construed as harassment;
- Transmitting spam or malicious content (viruses, spyware, malware);
- Violating copyright, license agreements or other contracts;
- Representing personal opinions as that of the organisation; and
- Forwarding any organisation or client information to personal email addresses.

Personal use (any access which is unrelated to official duties) of HSC email services is only permitted in accordance with local security policies. Personal use of HSC email shall be avoided where possible. Access is not permitted for commercial use.

Emails originating from the HSC email service shall have an automatically applied disclaimer appended to the body of the email. The disclaimer shall provide information such as:

- The Confidentiality / data classification that should be applied to the communication;
- Intended Recipient use only, and direction for where mis-transmission occurs;
- Views and opinions are those of the author, and not necessarily those of HSC;
- HSC Network monitoring may take place to ensure compliance with HSC Policies;

- HSC scans outgoing email, but takes no responsibility for malicious email content; and
- Potential Public disclosure of email communications under the Freedom of Information Act 2000 and GDPR legislation.

All staff are responsible for ensuring the confidentiality of information they send by email.

All personnel shall comply with the Information Security Data Transfer Standard when using email to transfer HSC information to others.

Personal data must not be sent by email outside the HSC network unless following agreed and documented processes that include the appropriate security measures, and as approved by the HSC ICT department such as file encryption or cloud based secure transfer services.

HSC Information Assets, including personally identifiable information, must not be emailed either to or from any staff member's personal email account.

All Staff must not arrange to auto-forward emails from their HSC account to other e-mail accounts e.g. @doctors.org @qub.ac.uk, or from their personal e-mail accounts to their HSC account.

Your HSC email account will contain sensitive information and that must be vetted before being forwarded on to any other email account. Auto-forwarding removes this vetting stage.

Refer to the local policy for details on email retention periods and maximum mail box sizes.

Phishing and Social Engineering

All staff shall be trained to identify phishing or social engineering email communications.

All staff must not interact with suspected or actual phishing / social engineering communications. If unsure of the validity of an email or any other communication, seek guidance from the local ICT Service Desk.

Particular attention must be given to emails, especially containing attachments, links or files, from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought from the local ICT Service Desk before any such email is opened.

Access to Another Individual's Mailbox

Unauthorised access to other user's E-mail accounts and mailbox is forbidden.

Where staff take periods of scheduled leave e.g. annual leave, term time etc. and there is a need to access historical emails, they should grant permission to the appropriate people. Guidance on how to do this is available from your local organisation IT Helpdesk.

If there is a business need to access another user's mailbox in circumstances such as sick leave or personal emergencies were an absence from work is unexpected, the request may be granted to the appropriate line manager. The line manager will firstly take reasonable steps to notify the employee that access is being requested for business reasons. This step is to inform the owner of the mailbox, not seek permission from them. Human Resources have approved view only access via this process and it is restricted to business related emails. Staff should note that it is not technically possible to prevent access to specific emails, e.g. personal ones, held within a mailbox where delegate access has been granted. Where these emails have to be retained moving them to a specific folder labelled Personal and or clearly marking them in the subject line as Personal should be considered.

When the employee returns, the authorising manager will inform the employee that their email account had been accessed by other individuals and the reason why this was necessary.

LIABILITY

The HSC does not accept any liability that may arise from employees using hscni.net email for personal use e.g. personal use of the email in response to spam, which may at a later stage result in fraud.

Staff should be aware that they might be personally liable to prosecution and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a person that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

Staff are further reminded that under Section 77 of the Freedom of Information Act 2000 it is a criminal offence after a request for information has been received under the Act to alter, deface, block, erase, destroy or conceal any record held by the HSC, with the intention of preventing the disclosure by the HSC of all, or any part, of the information to the communication of which the applicant would have been entitled. This clearly includes any E-Mail related to the request.

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.

APPENDIX 2

1.02 Removable Media All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

Removable Media by its very nature allows digital data to be removed from the controls of the HSC computer systems and moved internally and/or externally to HSC premises – this results in many risks to the security of HSC Data and ICT systems.

Removable Media is considered as digital storage that can be removed from a computer system and includes, but is not limited to:

- USB Storage, or Storage using a different hardware interface, (e.g. Flash Drives, USB/Thunderbolt External Hard Disks);
- Optical Media (e.g. CD's and DVD's);
- Memory Cards (e.g. SD Cards);
- Mass Storage Devices (e.g. Mobile Phone Storage, wireless storage devices);
- Tape Drives (e.g. Backup media.).

PURPOSE

This Information Security Standard is in place to ensure HSC organisations are able to use removable media 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 or NIFRS Information Assets and Systems.

SCOPE

This 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 and NIFRS, including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;

- Voluntary Health Sector organisations / Volunteers;
- 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.

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.

REMOVABLE MEDIA

Use of Removable Media

All HSC organisations must ensure that processes and standards are in place to govern the secure use, handling and destruction of removable media.

All staff should be aware that:

- Only organisation approved Removable Media Devices shall be used to store, download or transport organisation and client information.
- When Removable Media is needed to support the business, it shall be limited to the minimum amount of data and users required.
- Unknown removable media must not be connected to an HSC computer system (e.g. a USB Flash Drive found internally or externally to HSC Premises) but should, instead, be handed to the ICT Service Desk.
- Encryption must be used when storing HSC data on removable media. See Encryption Standard for more information.
- Portable Storage Media devices should be secured in locked storage overnight or when not in use in HSC's premises.
- All personnel shall comply with the Information Security 1.07 Data Transfer Standard when using Removable Media to transfer HSC information to others.

- Removable media should not be the primary or sole storage location for HSC information.
- All HSC organisations must ensure that processes and standards are in place to ensure backup copies of information are made and tested regularly. The requirement to backup, i.e. the information, the frequency and the extent, will be determined according to risk, regulation and business needs.
- Information governance activities (i.e. security controls, retention and handling procedures) must be considered and implemented, in addition to the Information Security Policy, throughout the data storage and backup processes.

Protecting HSC Devices

All staff shall ensure all necessary precautions are undertaken to protect HSC removable media, and the data stored, both internally and externally to HSC premises.

HSC equipment shall be used for HSC business purposes in line with local policy.

Lost or Stolen Information and Portable Storage Media Devices

All staff should report all data (electronic or hardcopy) and device losses (including portable storage media devices and any other firm equipment) to your line manager and your local ICT Service Desk and if applicable a DATIX incident must be raised.

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.

APPENDIX 3

1.03 Use of Internet Services All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

The internet is a global interconnected computer network allowing the majority of our digital devices and systems to communicate with one another, this allows us to access the world wide web, and share data with anyone in the world almost instantly. These uses of the internet are herein referred to as Internet Services. This level of interconnectedness has inherent risks, such as unauthorised individuals trying to gain access to systems that they don't have access to (hackers), malicious software (malware) that can infect our ICT systems and cause disruption to our organisations and social engineering enabled by the internet that can harm our people.

HSC Organisations need to understand these risks and ensure they take the right steps to protect HSC's people, Information Assets and Systems.

PURPOSE

This Information Security Standard is in place to ensure HSC organisations are able to use Internet Services 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 or NIFRS Information Assets and Systems.

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 and NIFRS, including:
    - HSC and NIFRS employees
    - Temporary Staff including agency and students
    - Voluntary Health Sector organisations / Volunteers
    - 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.

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.

USE OF INTERNET SERVICES

Connecting to the HSC Network

Where connection to the internet is required, all staff must connect HSC devices to the HSCNI network regularly to ensure information security controls, such as anti- malware software, are kept up to date.

Any out-of-date information security controls, that have not been able to automatically update, must be reported to the local ICT Service Desk.

A HSC device that has not been connected to the network for 3 months must be disabled from accessing HSCN resources. It may be reenabled upon the user contacting the ICT helpdesk who will ensure security controls are up to date.

Usage of Internet Services

All staff must use internet services in a secure, ethical and legal manner. Staff shall only use internet services for reasonable personal use as agreed with your line manager. Examples of prohibited Internet Services include but are not limited to:

- Attempts to gain unauthorised access to information resources;
- Accessing material that is pornographic, illegal, offensive, or discriminatory;
- Accessing non-approved file sharing services or software;
- Activities that could be damaging to the reputation of the organisation;
- Activities that interfere with business requirements; and
- Activities that violate copyright, license agreements or other contracts.

- The use of proxy avoidance

If access to a blocked internet service is required, staff shall follow their local ICT process to request access. Such access may be denied if a sufficient business reason is not provided, it is a prohibited use, or is deemed a significant risk.

Registering to internet services with a business email address is limited to business only and should not be used for any non-business use such as for personal items. For example, online shopping accounts and personal social media.

All personnel shall comply with the Information Security Data Transfer Standard when using Internet Services to transfer HSC information assets.
If there is a business requirement to purchase online goods or internet services, this must be done in accordance with the organisation's local procurement and approval process.

Social Networking and Blog Sites

Staff should follow their local organisations Social Media Policy. Examples of inappropriate use include, but are not limited to:

- Using HSC or any other organisation's brand on social media as their own;
- Using social media to the extent that it interferes with your responsibilities at HSC; and
- Using social media in a way that could be damaging to the reputation of HSC.

Involvement in Forums / User groups

Involvement in Forums / User Groups is permitted for business purposes only and must be authorised by your organisation. Any request for access to any of these forums should have approval of the respective Assistant Director/Director. When so doing, staff must not (unless specifically authorised to do so) speak or write in your organisation's name and must make it clear that their participation is as an individual speaking only for themselves and any comments are their personal opinion. In any such use of internet facilities, employees must identify themselves, with their own full name, honestly, accurately and completely. The misuse of such facilities may lead to disciplinary action when staff are acting in a personal capacity or even in a business capacity.

When participating in a forum / user group, staff **must**:-

- Refrain from political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service;
- give due regard to maintaining the clarity, consistency and integrity of the HSC corporate image and avoid making any inferences that may prove inappropriate

from an HSC perspective;

and **must not**:

- reveal sensitively marked information, client data, or any other material covered by HSC policies and procedures;
- Use HSC internet facilities or computing resources to violate applicable laws and regulations in any way or to compromise the security (including confidentiality) of HSC data.

Malware and Viruses

All staff should take all reasonable steps to ensure they are not responsible for the introduction of malware or unauthorised access to HSCN or HSC Information Systems. This includes, but is not limited to:

- Not opening files from unknown sources;
- Not downloading software from unapproved sources;
- Taking care when browsing the world wide web, such as using search engines results and visiting unfamiliar websites;
- Not entering HSC identification or authentication information to non-HSC managed Internet Services; and
- Not uploading HSC information to third party websites unless it is part of a contractual agreement with the third party, for example using a third-party online translation service to translate personal information where we do not have a direct and contractual relationship.

Inappropriate Material

Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature; whether in pictures, cartoons, words, sounds or moving images, whether or not purporting to be of a humorous nature. Staff should be aware that the decision as to what material is considered offensive can depend on the perception of the recipient and/or observer, rather than the intention of the sender. The final decision on what is offensive is determined by the local Director of Human Resources.

When a site containing inappropriate material is accessed, staff must immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such connections must be reported immediately to the **BSO ITS** Service Desk so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation.

Staff should be aware that where attempted access to a website categorised by the Internet Watch Foundation (IWF), e.g. child sexual abuse and criminal matters, is logged the BSO ITS will fully co-operate with the Police Service Northern Ireland (PSNI) to identify and take action against any employee.

All individual employees have a requirement to inform the PSNI immediately should they witness anyone accessing website material which may be categorised by the Internet Watch Foundation. These broadly include:-

- Images of child sexual abuse;
- Criminally obscene content;
- Incitement to racial hatred content.

LIABILITY

The HSC does not accept any liability that may arise from employees using the Internet for personal use e.g. personal use of the internet to complete an online transaction, which may at a later stage result in fraud.

Staff should be aware that they might be personally liable to prosecution and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a person that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

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.

APPENDIX 4

1.04 Asset Management All User Standard

INTRODUCTION

HSC 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.

PURPOSE

This Information Security Standard is in place to ensure HSC 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.

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, including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - 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.

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.

ASSET MANAGEMENT

Inventory of Assets

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

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 an HSC information System, with the clear distinction that it is externally managed.

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

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

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.

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.

Tools must be used to identify unauthorised hardware or software.

Ownership

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.

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

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

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.

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

Acquisition of Assets

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

Asset Selection and Approval

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.

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

PROTECTION OF ASSETS

End Users

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.

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.

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.

Staff must report all lost assets to Line Managers and BSO ITS department immediately.

System Owners

An appropriate set of procedures for information labelling must be developed and implemented. Procedures for information labelling must cover information and related

assets in both physical and electronic formats.

Controls in place to protect assets must be commensurate with the classification of the information stored on, processed or transmitted by the asset.

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.

BSO ITS 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).

Asset Handling

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.

STORAGE MEDIA HANDLING

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

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

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.

REDEPLOYMENT, DECOMMISSIONING AND DISPOSAL

End Users

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

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.

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

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.

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.

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.

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

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.

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

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

Records Management

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.

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.

APPENDIX 5

1.05 Clear Desk and Screen All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

A common source of information loss originates from information being left insecure and unattended in their work area. To mitigate this risk, the confidentiality and integrity of information must be ensured when staff are not physically present. A further risk occurs when using computer screens, as overlookers could have visual access to information that they should not have access.

PURPOSE

The purpose of this policy is to protect HSC information from unauthorised disclosure, loss or damage. It establishes minimum requirements for a clear desk and screen environment, addressing the protection of hardcopy information, removable media and on-screen information.

SCOPE

This 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, including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - 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.

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.

CLEAR DESK AND SCREEN

PHYSICAL ENVIRONMENT

Desk and Office Environment

All staff must ensure personal information or business sensitive information is not left in view or unattended at any time. This includes personal information or business sensitive information contained within hard copy documents or notes left on desks, printers, on top of filing cabinets etc. in addition to being visible on computer screens. Where the use of screen reading software for employees with sight loss is required, headphones or a private area must be provided to avoid potential disclosure of personal or confidential material.

When hard copy information is no longer required, all staff must either dispose of or secure the information (e.g. secured in a locker or shredded).

Ensure digital content on screen is not available or accessible to others when not attended (e.g. use a privacy screen during use and locking the screen when unattended).

Staff must make use of collaboration equipment, including but not limited to whiteboards, flipcharts, post-it walls, in a manner that ensures the protection of any personal information or sensitive business information. This may be to use the equipment out of view of unauthorised individuals and erasing the content when it is no longer required or is to be left unattended, unless it can be secured and made non-visible.

Portable devices, such as mobile phones, that contain personal information or business sensitive information must be secured in line with local device policy, including but not limited to the use of encryption, a strong passcode, and not leaving

the device unattended or unlocked.

Workplace furniture shall be positioned so that personal information or business sensitive material is not visible from either the windows or the hallway. Where this is not possible, compensating controls, such as closing blinds or using privacy screens, must be implemented.

Equipment in public areas must be locked with an approved locking cable or locked away in a drawer when left unattended.

Where audio or video conferencing is used, it should take place in a non-public area with staff avoiding personal information or business sensitive information being seen or heard by unauthorised individuals.

Staff must only store information in hardcopy form if absolutely necessary. Where appropriate, documents should be scanned, or information transferred, and stored digitally within an appropriate HSC Information System. Hardcopy versions must be disposed of in line with local record management policies and procedures.

Where information is stored in hardcopy form, it must be stored in line with the local Records Management Policy. Staff must label the information in accordance with the local classification policy, and store it in a way that is commensurate to the classification of the information.

Use of Locked Areas

Staff must securely store hardcopy information in a locked location inaccessible to unauthorised individuals when it is not in use or when it is left unattended.

Where lockable cabinets are not available, staff must store paper and removable media out of sight in a room which is locked when left unattended.

Locked areas must be secured when not in use or unattended.

Staff must store cabinet and cupboard keys securely, preferably in a combination safe or cabinet. Keys must not be left in locks.

Printers and Photocopiers

Staff must only print personal information or business sensitive information if it is in line with the execution of their official duties and in accordance with local policy.

Staff must remove printouts, especially those containing personal information or

business sensitive information, from the printer immediately.

Where applicable, access controls must be implemented on printers, fax machines and photocopiers to ensure staff are present during the print process.

COMPUTER ENVIRONMENT

All staff must protect authentication information and devices from unauthorised disclosure.

Staff must not leave removable media unattended.

Staff must lock devices when leaving them unattended, and automatic time-out screen locks must be enabled.

Digital Information Systems must be configured to identify and authenticate users, in accordance with the Accounts and Password Policy.

MONITORING

Staff must be aware that any data on the organisation's systems and equipment 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.

HSC may at any time, and without notice, conduct clear desk and screen compliance checks or audits, and may remove any information or equipment that is in breach of this policy. All users must co-operate fully with any such audit.

APPENDIX 6

1.06 Cloud Security All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate security controls, it can also expose individuals and HSC organisations to online threats such as data loss, theft, and unauthorised access to HSC networks. The governance of cloud computing solutions is therefore essential to protect the integrity and confidentiality of HSC data and ensure the security of HSC systems and networks.

Cloud computing is a shared technology model where responsibilities for different elements of the model are distributed across multiple organisations. As a result, security responsibilities are also shared.

PURPOSE

The purpose of this Standard is to outline good governance and security practices in relation to the use of cloud computing solutions across HSC and NIFRS organisations.

SCOPE

This Information Security Standard applies to:

- All parties who have access to, or use of systems and information belonging to, or under the control of, HSC and NIFRS including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - Third Party Contractors; and
    - Any other party making use of HSC ICT resources.
- Information stored, or in use, on HSC ICT systems;

- Information in transit across the HSC network;
- Information leaving the HSC network;
- 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.

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.

CLOUD SECURITY

Risk Management

Prior to acquiring a cloud service, HSC organisations must analyse the risk associated with adopting the cloud-based solution, and plan for risk treatment and risk control activities associated with the service.

To effectively manage the information security risk of a cloud service, HSC organisations must ensure risk management requirements are established and actioned in line with the Risk Management, Information Security Policy and Information Security Standards

HSC organisations must ensure the assignment of risk management responsibilities to all organisations involved in the design and build of the cloud service. Internally, the organisation must further assign responsibilities to the relevant HSC staff.

HSC organisations must ensure a cloud service tolerance for risk is established and communicated within their Service-Level Agreements (SLA), including information on any decision-making activities that may impact the risk tolerance.

HSC organisations must conduct risk assessments associated with cloud information governance requirements at planned intervals, considering:

- The awareness of where sensitive data is stored and transmitted across cloud applications, databases, servers, and network infrastructures;
- Compliance with defined retention periods and end-of-life disposal requirements; and

- Data classification and protection from unauthorised use, access, loss, destruction, and falsification.

HSC organisations must ensure near real-time monitoring, alerting, and understanding, by each organisation involved, of the information security risks arising from the operation and/or use of the information system leveraging the cloud service.

HSC organisations must ensure accountability by all organisations involved and near real-time information sharing of the organisations' incidents, threats, risk management decisions, and solutions.

Data Assessment

HSC organisations must understand the types of data that will be traversing cloud services. To support this and to understand the risks associated, organisations must:

- Specify and manage all acceptable data types/attributes that can be collected, stored or processed by cloud services;
- Data flow mapping should be performed to understand the movement of data, e.g. HSC, third party cloud service providers, and where data is located geographically;
- Quantify how much data is under consideration;
- Define how long data types can be held within cloud services;
- Carefully assess the data types/attributes and decide which each relates to;
- Retain the list of acceptable data types/attributes and record the rationale for selecting each;
- Ensure these requirements are completed in line with any local Information Classification Policies, Retention Policies or Data Privacy Policies; and
- Ensure data privacy procedures are followed, e.g. completing a Data Privacy Impact Assessment (DPIA).

Contracts

All Cloud contracts need to be robust, compliant with relevant law and in line with any local Third-Party Management Policies. HSC organisations must have documentation that details the duties and obligations that have been agreed.

Availability

HSC organisations must clarify what the Cloud Service Provider defines as downtime and ensure it is scheduled contractually, aligns with organisations availability

requirements and does not conflict with its business hours.

HSC organisations must confirm what type of service monitoring and alerts are available, and include the ability to terminate the contract without further liability if uptime falls outside of the agreed parameters.

HSC organisations must include requirements that affirm the Cloud Service Provider's business continuity plan, specifying redundancy requirements to contain, at a minimum, data backup and recovery methods/infrastructure/processes.

HSC organisations must require the Cloud Service Provider to certify that it will participate with the organisation in disaster recovery testing at specific time intervals (e.g. every two years).

Compliance Requirements

HSC organisations must review the Cloud Service Provider's T&Cs and ensure they are compliant with the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR).

HSC organisations must ensure Cloud Service Providers hold the necessary standards and certifications to comply with applicable laws and security standards when processing, storing, transmitting or maintaining confidential HSC data (e.g. ISO27001, ISO27017 or Cyber Essentials Plus).

HSC organisations must ensure data is only to be transferred (in this context accessed or hosted) within a country or group of countries as permitted by the Data Protection Act and/or relevant legislation. Further guidance is available from the Information Commissioner's Office.

Data Access

HSC organisations must confirm how data access can be limited by the Cloud Service Provider's service, including a review of:

- The different user permission roles offered;
- The various accessibility parameters for each role and the administrator's access rights; and
- Ensuring all user actions can be tracked.

HSC organisations must contractually prohibit Cloud Service Providers from sharing confidential HSC data with anybody other than approved third parties that are required to provide services.

HSC organisations must ensure they are able to access their data on demand, ideally on a self-service basis, (at any time) and in the requested format.

Data Breach or Loss

HSC organisations must require Cloud Service Providers to inform the organisation immediately if a potential or actual data breach has occurred in line with the DPA 2018 or GDPR, any local incident management policies and data privacy policies.

HSC organisations must define who is accountable for the loss of data in transit or at rest.

HSC organisations must ensure Cloud Service Providers can provide appropriate and timely support for computer forensic investigations and analysis as part of the contract.

Termination and Disposal

HSC organisations must confirm the Cloud Service Provider is compliant with HSC's local policies for data storage and disposal.

HSC organisations must require the Cloud Service Provider to apply a mandatory data wipe-out and sanitisation under the HSC organisations' review and approval upon contract termination or expiration.

HSC organisations must establish an exit strategy with terms that trigger the retrieval of HSC assets and data in a specified time frame.

CLOUD SECURITY PRINCIPLES

HSC organisations should take a risk-based approach to managing information security in the cloud. The approach should be informed by the data assessment, risk assessment, and cloud service model selected. HSC cloud services and transiting networks must be adequately protected using a combination of network security controls and considerations made to ensure compliance with applicable regulations and laws.

Cloud Design and Build

Ahead of any new cloud system development, or significant change to a cloud system, HSC organisations should develop a cloud system design to determine the desired outcomes of using the cloud service, security and privacy by design requirements, conducting a feasibility assessment (taking into account legal framework conditions), the maturity of the HSC organisation and changes that are required to adapt internally

for the cloud service deployment – in addition to the Data Assessment and Risk Management as previously described.

After data assessment and risk management, the cloud service model selection must take place. The shared responsibility model will differ (Figure 1) depending on the selected cloud service provider. Figure 1 below shows where HSC (green) or the CSP (blue) is responsible for ensuring that a specific responsibility is met.

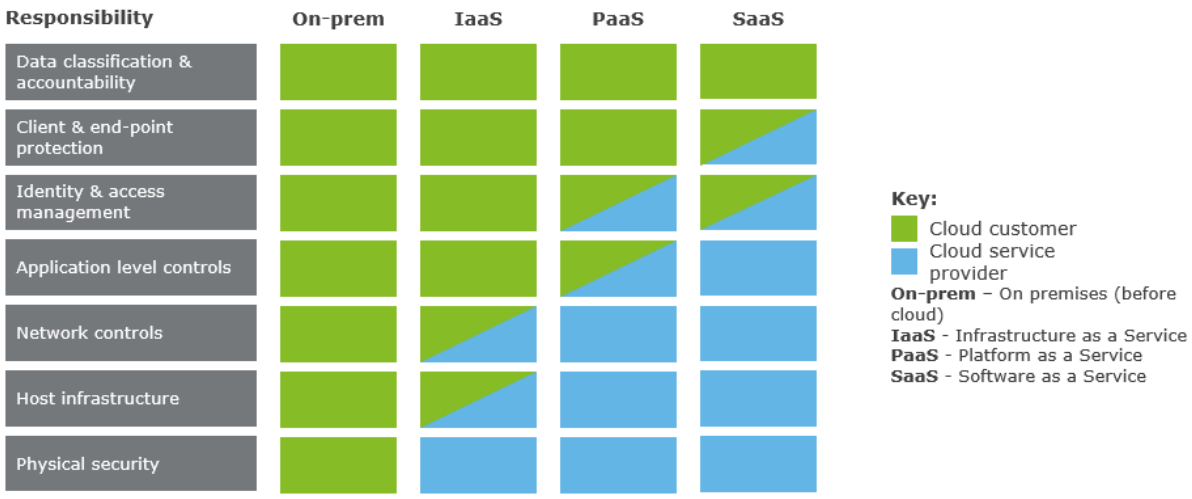

Figure 1 – Source: Shared Responsibility for Cloud Computing (Microsoft)

HSC organisations must use a security-hardened master operating system image to build virtual machines, in line with NCSC End User Device (EUD) build guidance.

HSC organisations must ensure that there is an appropriate network design that can protect HSC data (e.g. having a DMZ and network segmentation).

Security Controls

HSC cloud-based information assets (including information systems) processing (collection, recording, using, storing, etc.) HSC data must be adequately protected against unauthorised access, corruption, failure or loss.

Cloud services must be secured to prevent data loss, theft or compromise, including that held on backup media. In addition to secure configuration being applied, cyber security controls should also be added as required, including:

- Firewall (both network and web application);
- Intrusion Prevention/Detection systems;
- Anti-malware software;
- Data Loss Prevention;

- Distributed Denial of Service Prevention.

HSC organisations must utilise strong cryptography to encrypt cloud data, whether the data is at rest or in transit. Cryptography/encryption standards should be utilised as defined by industry standards such as NIST SP800-57 or ISO27017:2015 and ISO27018 and managed in line with the Information Security Encryption Standard.

Physical security of premises used as cloud data centres and the equipment they utilise for HSC data must be required as part of any contract, this should include physical access controls, security measures and CCTV systems.

Assurance must be sought regularly (at least annually) from the Cloud Service Provider (CSP) that they have adequate controls in place to protect HSC data.

HSC organisations must ensure CSPs have controls in place to ensure their clients cannot access one another's data, and to prevent a new client from seeing data left behind by a former client.

Secure authentication methods must be used for ICT administrative staff and access controlled depending on risk and business justification. A suitable auditing solution must be in place to record all ICT admin access rights and their use of that access to data and hosting environments.

HSC organisations should use access controls such as:

- Regularly updated Role Based Access Control;
- Joiners, movers, leavers processes;
- The 'principle of least privilege' enforced using access control tools and processes, including for privileged access;
- Multi-factor Authentication to obtain access to the system;
- Capturing and regularly reviewing logs of access attempts to identify unusual behaviour.

The methods used by CSP's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service and/or HSC information.

HSC organisations are responsible for the administration of resources and systems they have chosen to securely deploy onto cloud services.

Data Transfer and Information Sharing

HSC organisations must ensure physical location and jurisdiction requirements are understood and implemented, for example, when using cloud services based outside of the UK. See the Information Security Data Transfer Standard for more information.

Resilience Activities and Monitoring

HSC organisations must design for failure. Solutions should be architected for cloud such that they are resilient regardless of the underlying cloud infrastructure. For example: HSC organisations can achieve this by:

- Using multiple availability zones/data centres;
- Have resilient network links to each zone/data centre;
- Using different cloud vendors or multiple regions from the same vendor;
- Having resilient network links to each region/vendor; and
- Ensuring their system has adequate DDoS protection in line with HSC risk appetite. This may be provided by the CSP or a third party.

HSC organisations must implement monitoring solutions, in line with the HSC risk management framework, to identify and defend against attacks. For example, this could include real-time Security Incident and Events Management (SIEM) tools.

HSC organisations must be provided with the audit records by the CSP which are needed to monitor access to the cloud service and the data held within it.

HSC organisations must ensure preparations have been made to enable a prompt, coherent and well-practiced incident response and recovery. Refer to the Information Security Incident Identification and Reporting Standard for more detail.

All staff must report any actual or suspected security incident as soon as they are aware of it and do so in line with organisational policies.

Examples of cloud security incidents that require reporting include but are not limited to actual or suspected:

- Breaches of confidentiality or cloud security;
- Unauthorised access or changes to cloud services, configurations and resources;
- Compromise of a password or login; and
- Compromise of a CSP.

Business continuity and incident response plans shall be subject to testing at planned intervals (at least annually or upon significant organisational or environmental changes).

In the event of CSP outages, HSC organisations must adhere to requirements outlined in their local Business Continuity Policies. These include, but are not limited to:

- HSC shall prepare for CSP outages;
- Considering options for portability in case HSC need to migrate providers or platforms; and
- Have backup processes and solutions in place for critical procedures.

Governance

The CSP must have an adequate governance framework in place, this includes the management of the service, risk management, incident management, processes and procedures, roles and responsibilities, suitable technical controls, and they are able to ensure compliance with applicable legal and regulatory requirements.

Recognised standards can be used by HSC organisations to provide assurance against this framework, for example CSA's STAR programme or ISO/IEC 27001. Refer to local Third-Party Management Policies for more details.

Ensure there are sufficient contractual requirements with the CSP to ensure this Standard (and any supplementary and appropriate Policy, Standard or Control) is upheld.

HSC's data retention requirements (as set in the Information Governance Policy) must be supported by the CSP.

HSC organisations must have appropriate system and service acquisition policies and processes, robust enterprise risk management regimes and the ability to mitigate, operate or terminate services if required.

HSC organisations must ensure that changes to a cloud system have been managed in accordance with change management procedures and are properly authorised and tested. Changes should be assessed to ensure security controls are not inadvertently made less effective.

The CSP must ensure that its supply chain meets the demands of the contract in place with HSC and required security principles are implemented as required. This can be

assessed through the application of appropriate standards and certifications such as ISO/IEC 27001, or ISO/PAS 28000:2007.

Security Testing and Patch Management

HSC organisations must undertake regular (at least annually or upon a significant change to the cloud service design, infrastructure or configuration) security testing for cloud systems and associated controls and processes. Depending on the risk assessment, testing could involve vulnerability scanning, penetration testing, or a combination of the two and the subsequent management of any findings. HSC organisations must ensure:

- The test is scoped appropriately for the level of risk posed by the cloud service and it is conducted by a suitably qualified provider, such as those certified under the CHECK scheme.
- Scoping should include data in transit, host operating system, physical components and network devices, application security etc.

HSC organisations must undertake an annual assessment against a recognised standard, such as Cyber Essentials Plus, to test the security of the service. This test must be conducted by a suitably qualified provider certified under the CHECK scheme.

Patch management must define the tools, analysis processes and remediation practices to ensure patches are deployed within appropriate timescales (depending on risk) across the cloud service.

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.

APPENDIX 7

1.07 Data Transfer All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

Data Transfer is the process of moving HSC information from one place to another. It could be physical movement of hard copy information, e.g. sending documents via a courier service, or digitally transferring electronic information, e.g. sending a spreadsheet via email.

Risk to the security of the Information increases where HSC organisations transfer data, for example where we rely on transfer mechanisms outside of our Information Security controls to move the information, or as legal considerations become applicable, such as transferring information internationally.

PURPOSE

The purpose of this Standard is to provide clear guidance on transferring information. This Standard aims to reduce the risk of any data security breaches across the organisation by ensuring the confidentiality, integrity and availability of information during the transfer or sharing processes.

SCOPE

This 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, including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - 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.

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.

DATA TRANSFER

Transferring and Sharing Personal Data

Based on the information classification assigned to data, and according to local Data classification Policies, all staff must ensure the following:

- All other HSC Policies and Standards are complied with.
- HSC Data Access Agreement (DAA) template should be completed where personal identifiable data is shared for a secondary purpose (e.g. not for direct care or for a reason other than the initial purpose for which the data was collected)
- Personal data and/or confidential information is only transferred to those who are authorised to receive it.
- Information is relevant and accessed/transferred on a need-to-know basis.
- The impact to HSC and any third parties is considered before disclosing information, and where personal data, potential harm to the data subject is considered.
- Information shared is sufficient for its purpose and is of the right quality to ensure that it can be understood, used for its intended purpose, and relied upon.
- Information is accurate prior to sharing, it is up to date and clearly distinguishes between fact and opinion. If information is inaccurate, incomplete or out of date then this must be escalated in line with a local Records Management Policy.
- Third party Data Transfer processes are not fully initiated until both organisations are aware and assured on the level of security and confidentiality through a Data Sharing Agreement (DSA).

Where a data set contains data of multiple classification levels, the requirements of the highest classification shall be used for all data in the same transmission (for example, 20% of the data is sensitive personal data, and 80% is not, 100% must be treated as sensitive personal data, or the data must be split into separate transmissions).

Staff must stay vigilant when receiving requests for information and look for signs of phishing or social engineering attack. If in doubt, staff must check with the requester using a trusted (alternative) communication method, and follow correct process before sharing information, especially if there is an unusual or greater time pressure than normal to the request.

Organisations disclosing information containing personal data will be subject to the Data Protection Act 2018 (DPA 2018). Disclosure of personal data is an act of 'processing', so any disclosure containing personal data must comply with all of the provisions of Part 3 DPA 2018 or the General Data Protection Regulation (GDPR).

HSC staff must consider the following prior to sharing personal data outside of an agreed process:

- What is the sharing meant to achieve?
- What information needs to be shared and is it proportionate?
- What HSC classification is the data, do any special measures apply?
- What risk does the data sharing pose to individuals?
- Are we allowed to share the information?
- Is the data being shared with a third party, if so is a data sharing agreement in place?
- What would happen if we did not share the data?
- Who requires access to the shared personal data?
- Does this contain any special category data?
- When should it be shared?
- How should it be shared?
- Do we need to record the decision to share?
- How can we check the sharing is achieving its objective?
- Could the objective be achieved without sharing the data or by anonymising it?
- Will any of the data be transferred outside of a country or group of countries as permitted by the Data Protection Act and/or relevant legislation?

- Do we need to review the DPIA?

In addition to the DPA 2018 and GDPR requirements, the 'Confidentiality: NHS Code of Practice' describes the following four requirements that must be met when handling confidential patient information:

- Protect – look after the patient's information;
- Inform – ensure that patients are aware of how their information is used;
- Provide choice – allow patients to decide whether their information can be disclosed or used in particular ways; and
- Improve – always look for better ways to protect, inform, and provide choice.

Third party transfers requesting disclosure of personal information from HSC organisations, must be approved by the Personal Data Guardian (PDG). Once sharing has been approved, the DSA must be developed and signed by both organisations, confirming their assent to the Data Transfer process.

The PDG, on behalf of HSC, reserves the right to reject an individual exchange of any personal data should they not be fully satisfied with the security and confidentiality procedures of a third party organisation, irrespective of the DSA.

If disclosing personal data, under the DPA 2018 and UK GDPR staff must ensure:

- A Data Protection Impact Assessment (DPIA) has been completed, and is up to date, for the business process;
- Personal data is disclosed for the same specific purpose for which it was originally collected;
- Disclosure is necessary and in-line with the purpose for which it was originally collected;
- Unless there is a legal basis for processing or sharing information, it should be shared with the consent of stakeholders. For consent to be given, stakeholders must be informed of the purposes for which the information about them may be recorded and shared;
- Reasonable steps are taken to ensure that no inaccurate, incomplete or out- of-date personal data is disclosed;
- The recipient is provided the information necessary to allow them to assess the degree of accuracy, completeness and reliability of the data. Particular care must be taken with bulk disclosures;
- That if it is subsequently discovered that the data was incorrect or the transmission was unlawful, the recipient is notified without delay; and

- Engagement with the Data Protection Officer before any potential international transfers of personal data outside of country or group of countries permitted by the Data Protection Act and/or relevant legislation.

A record of data sharing must be kept, identifying the content shared, how it was shared and the protection applied, when it was shared and that receipt of the transfer has been successful at the destination.

Data Protection Impact Assessment (DPIA)

Before establishing any new form of data transfer process that involves personal data, a DPIA must be conducted as a requirement under the DPA 2018/GDPR. The DPIA initially has screening questions to assess whether there is a high risk, and if so, the full DPIA must be completed.

Any new data flows that arise out of a new project or procurement where HSC is the data controller or receives personal or sensitive information as defined within the Information Classification scheme will need to be recorded as part of HSC's Asset Register. Refer to the Information Security 1.04 Asset Management Standard (Appendix 4) for more information.

Data Sharing Agreements (DSA)

All HSC organisations must establish DSAs when transferring HSC data between the organisation and third parties. The following information must be captured:

- The details of the two parties entering into the DSA;
- A brief description of the background and context of this data sharing agreement;
- Details about why the personal data is processed?
- Details of whose, what and how personal data is to be shared / processed, and a map of the data flow;
- The specific basis for processing by each party;
- The relationship in terms of data controller / data processor roles;
- How the parties intend to have in place appropriate technical and organisational security, retention and disposal measures;
- How security incidents or data breaches will be handled;
- Review/termination details for the DSA;
- Declaration, indemnity and governing law and jurisdiction details.

The DSA shall require that the third party must:

- Act only on instructions from the HSC organisation;
- Ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality;
- Assist the HSC organisation by any appropriate means to ensure compliance with the rights of the data subject under Part 3 of the DPA, or the UK GDPR;

At the end of the provision of services:

- Either delete or return to the controller (at the choice of HSC organisations) the personal data to which the services relate; and
- Delete copies of the personal data by a secure method set out by the HSC organisation, unless subject to a legal obligation to store the copies.
- Make available to the HSC organisation all information necessary to demonstrate compliance with this section;
- Allow for and contribute to audits, including inspections, conducted by the HSC organisation as a controller or another auditor mandated by HSC; and
- Comply with the requirements of this section when engaging sub-processors.

HSC organisations must review DSAs on a regular basis to address any changes in circumstances and reassess the rationale for the data sharing activities.

DSA can only be approved by a Personal Data Guardian for the organisation who owns the information. If there is any doubt about whether information should be stored or disclosed, staff should speak to the local Data Protection Officer or a local Information Management specialist.

SPECIFIC CONSIDERATIONS WHEN TRANSFERRING DATA VIA DIFFERENT METHODS

Transfers of Data via Email

Any correspondence sent or received via HSC's email system is considered a public record and will fall under the requirements of the following:

- The Freedom of Information Act 2000 (FOI) in relation to business information;
- The DPA or the UK GDPR in relation to personal data.

All staff are responsible for ensuring the confidentiality of information they send by email.
Personal data must not be sent by email outside the HSC network unless proper security measures, approved by the HSC ICT department, are in place, including encryption or cloud based secure transfer services.

Where encryption is applied, the encrypted file and password should not be sent by the same route (e.g. if the data file is sent by email then the password must not be sent by email and should instead be sent by SMS text or a phone call) and the password must satisfy requirements within the Information Security Accounts and Password Standard (Appendix 11).

Personal data must not be emailed either to or from any staff member's personal email account.

Personal data must not be transferred to, stored or processed on any personal device.

The following specific safe email transmission procedures must be followed as a minimum:

- Staff must only send the minimum information required and care must be taken to ensure the correct email address is used, e.g. when using the 'reply to all' button, that information is sent to appropriate person(s);
- Staff must not include names, addresses or other identifiable information in the subject line of an email; and
- Staff must not share confidential information, i.e. special category data, as free text, for example directly in the body of an email. Staff shall share the information within a separate document (e.g. MS Word document) and send as an attachment that has been encrypted in line with the Information Security Encryption Standard (Appendix 8). Staff must comply with the process and if unsure, must seek advice from the ICT department on how to encrypt a document.

Physical Media Transfer

Any media containing information needs to be protected against unauthorised access, misuse or corruption during transportation (unless already publicly available). The following shall be considered to protect media when being transported:

- Packaging must be sufficient in order to protect the contents from any physical damage during transit;
- Logs shall be kept, identifying the contents of the media and the protection applied.

Transfers of Data via Removable Media

- All staff must be aware of the risks associated when removable media is used for data transfer. Refer to the Information Security Removable Media Standard for more detail (Appendix 2).
- Staff must ensure only approved encrypted removable media adhering to an appropriate level of encryption, as defined in the Information Security Encryption Standard (Appendix 8), are used for the transfer of personal data or business sensitive information.
- Staff must ensure removable media that has been approved for use within the organisation is appropriately labelled in line with the requirements of the classification of that data.
- Staff are not permitted to save the contents of organisation-encrypted devices onto personal devices (e.g. their home computer, laptop, smartphone or tablet) or other media.
- Staff must only use removable media to temporarily store and transfer organisation information that is required for a specific business purpose where the use of a more secure method is not available.
- The use of removable media by all sub-contractors or temporary workers must be risk assessed and be specifically authorised by the ICT department.
- See Transfers of Data Via Courier Services section for sending removable media via courier.

Transfers of Data via Cloud, Internet Services and Data Sharing Portal

- Staff and contractors must not introduce or use any cloud service providers (e.g. Dropbox, iCloud) to transfer data other than those provided or explicitly approved for use by the organisation, for example OneDrive using HSC credentials.
- Line managers, in collaboration with the local ICT Department, shall be responsible for the day to day management and oversight of data sharing within HSC approved cloud, internet storage and data portals.
- Only staff and contractors who have an identified, approved and agreed business need shall use cloud services for storage and data transfers.
- The storage or transfer of data between secure cloud providers by sub-contractors or temporary workers must be risk assessed and be specifically authorised by the local ICT department.
- Where the HSC secure cloud storage is being used for data transfer, the data must not be made available for longer than 72 hours (3 days) and must then be

removed entirely from the online service. This is to prevent data leakage from someone compromising a cloud storage account.

Transfers of Data via Courier Services

- HSC organisations must ensure only approved routine courier services, as defined by local process, are used for the transfer of non-personal or non-sensitive business information.
- HSC organisations must ensure only approved secure courier services, as defined by local policies, are used for the transfer of personal data or business sensitive information. Packaging must be sealed, tamper-proof and tamper-evident.
- Staff must obtain the appropriate level of authorisation prior to the use of a courier service, as defined by local policy.
- Care must be taken to ensure that information, other than the information required for delivery, for example the recipient's name and address, is not accessible without breaking the seal of the envelope/package, i.e. sensitive information visible through the clear window of an envelope.
- Specific processes must be created for frequent data transfers via courier.
- Where removable media is being sent via courier, the media must be encrypted before transport with the decryption password sent via a different method, for example if the removable media is sent by courier then the password must not be sent by courier and should instead be sent by email, SMS text or a phone call) and the password must satisfy requirements within the Information Security Accounts and Password Standard.
- The packaging used for transit must ensure that the contents is sufficiently protected from any physical damage likely to arise during transit, for example physical damage caused by dropping the package or water ingress.
- Recorded/tracked services should be used to confirm delivery.

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.

APPENDIX 8

1.08 Encryption All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

To ensure the security of HSC's information, it's important to have information security controls in place for our data and devices - encryption is one such control. Encryption converts the original data to a non-readable format that is accessible only to authorized parties who can unlock and decrypt to view the original data.

This information security control provides a high level of protection to devices, digital files and internet communications to minimise risks to the Confidentiality, Integrity and Availability (CIA) of HSC digital information assets and systems.

Cryptographic controls can also be used to achieve a number of information security-related objectives, including:

- **Confidentiality** – ensuring that information cannot be read by unauthorised persons;
- **Integrity** – proving that data has not been altered in transit or whilst stored;
- **Availability** – ensuring that information is only available to those who authorised to access it;
- **Non-repudiation** – proving that an event did or did not occur.

PURPOSE

The purpose of this standard is to inform HSC organisations of the minimum requirements, specific to encryption, when it comes to protecting the Confidentiality, Integrity and Availability (CIA) of digital information. Where necessary, it may be appropriate for local organisations to exceed this Standard and/or provide additional guidance on the implementation of encryption.

SCOPE

This 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, including:

- HSC and NIFRS employees;
- Temporary Staff including agency and students;
- Voluntary Health Sector organisations / Volunteers;
- 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.

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 (Appendix 9).

ENCRYPTION

Management of Encryption at HSC

Encryption techniques, deployed throughout the information lifecycle, must be a mitigating control whether data is at rest (i.e. data contained within a hard drive, computer, laptop, mobile device flash drive, or in a backup) or data is in transit (i.e. data that is flowing between devices, whether via an internal network or untrusted network/via the internet) where:

- Information classified as personally identifiable or business sensitive is being processed or shared using a digital device(s), including:
    - HSC computer systems, and mobile and tablet devices
    - Protection of secret authentication information (e.g. passwords, cryptographic keys and pins);
    - Electronic transaction data (e.g. payment information, credit cards etc);

    - Where local laws or regulations mandate;

- Digital devices and/or storage media has the potential to store personally identifiable information;
- Digital data is being shared over an untrusted network (a network that HSC has no control or assertions as to it level of security i.e. the internet);
- Digital data is being transferred using storage media (such as physical hard drive, backup media, USB memory sticks, SD cards, optical media etc.); and
- As otherwise identified as necessary by a risk assessment.

The encryption techniques used must have the strength and quality required to protect the confidentiality, integrity, and availability of information, as determined by:

- The risk posed by the data, i.e. personally identifiable or business sensitive information would require enhanced encryption techniques compared with potentially lesser encryption requirements for lower classifications.
- The type of processing being carried out; and
- Whether there are additional controls in place to protect the information, for example the data will not leave the internal network and there are other cyber security controls in place.

Where the use of approved cryptographic controls is not feasible (e.g. if prevented by local laws and regulations), appropriate compensating controls must be determined by the local risk and governance forum.

The impact of using encrypted information should be considered when implementing, for example malware detection or content inspection.

Controls preventing the malicious use of encryption must be in place to protect HSC and selected based on risk assessments to the HSC Network (HSCN), for example blocking encrypted file downloads that could contain malware, or blocking outbound VPNs that a malicious user or malware could take advantage of).

Third party suppliers and outsourcing arrangements should follow the scope of this standard. Deviation from this shall be subject to risk assessment and senior management should satisfy itself, as far as is reasonably practicable, that the systems and controls which are in place are appropriate to monitor and mitigate risk.

Staff who process personally identifiable information or sensitive business information must be trained to encrypt data appropriately.

Where data transfer of encrypted information is occurring outside of the UK, national laws, regulation and restrictions must be considered.

Technical Encryption Requirements

Where encryption is required, FIPS 140-2 is the minimum standard of encryption that must be applied. For example, all HSC laptops must be encrypted with full disk encryption compliant with FIPS 140-2, utilising the AES encryption algorithm and a 256-bit key.

Smartphones, tablets or similar mobile devices must be encrypted utilising full disk encryption.

Bring Your Own Devices (BYOD) are not permitted.

All portable storage devices which contain or have the potential to contain personally identifiable information/data will be encrypted, this will include portable hard drives, memory cards and USB mass storage devices.

Taking photographs with a digital camera (including unencrypted smartphones, tablets etc.) that uses either internal memory or removable memory is unlikely to be encrypted, or be able to be encrypted by the device. As photographs may contain personally identifiable and/or sensitive business information, all images must be removed from the memory card as soon as is practical (i.e. transferred immediately after taking the photograph(s) and before transporting the device) from memory cards and stored on the HSC Network (HSCN) immediately after being taken. At no time should images be retained and stored on memory cards and a secure deletion / full overwrite format should occur.

Where optical media (i.e. CD or DVD) is being used, the data stored on this media must be encrypted (either within an encrypted container or the file encrypted itself) if it contains personally identifiable information or sensitive business information.

Remote access to Trust networks must be channelled through the BSO secure VPN, site to site VPN or HSCN, all of which utilise end to end encryption.

Transfers across the HSCN or to other HSC organisations using web applications must use HTTPS/SSL.

Email Specific Requirements

Emails must be encrypted using a minimum of TLS v1.2 between trusts.

Encryption must be applied to transfers of personal/sensitive information via email, except email addresses within the following domains:

- .hscni.net',
- .n-i.nhs.uk
- '.nhs.uk'
- '.ni-gov.uk'
- .nihe-gov.uk
- .cjsm.net

HSC has agreed processes that cover all types of domains that must be followed when sharing information via email. **Further guidance should be sought from BSO ITS when required.**

Managing Electronic Keys

BSO ITS is responsible for the management of encryption keys on behalf of NIPEC. A key management system is used by BSO ITS requirements for:

- Generating, distributing, activating, storing, maintaining or changing keys;
- Including those issued by a certification authority and their continual upkeep;
- Issuing and obtaining public key certificates;
- Changing or updating keys including the frequency that keys should be changed;
- How to handle a compromised key(s) or recovering keys that are lost or corrupted;
- Withdrawing, deactivating, revocation and destroying keys;
- Back-up and archival of keys; and
- Key management logging and auditing.

HSC ICT's centrally approved encryption solutions will be used, and all encryption keys, passwords, passphrases or other keys must be held centrally. This is to ensure data is recoverable, should a key be lost or compromised.

Only encryption tools approved by BSO ITS may be used on HSC devices. These tools may vary between HSC organisations.

Portable devices should be procured with encryption in place e.g. memory sticks, portable hard drives.

Formal processes and standards must be established and regularly reviewed to protect cryptographic keys from unauthorised access, modification, loss or destruction at all stages of the key lifecycle.

A risk assessment must be carried out to understand the risks associated with the cryptographic lifecycle, including any potential failings within the lifecycle. If any risks are accepted via the local risk and governance forum, a plan must be established to uplift the capability to an approved standard within an acceptable time frame.

Keys for long term storage and other purposes should have a limited life span and be replaced at an agreed timeframe.

Keys for sessions and transactions should have a lifetime of no longer than is required to carry out the intended function, excess lifetime allows a higher risk of attack.

Activation and deactivation dates for keys must be defined to reduce the likelihood of improper use.

Electronic distribution of symmetric keys must be done using an encrypted, authenticated and time-stamped channel that protects the keys from compromise.

PKI infrastructure must use an offline, and stand-alone, root certificate authority (CA), which adheres to NCSC guidance.

Access to both the root and issuing CA and Registration Authority (RA) must be protected by appropriate access controls to ensure only valid, authorised, users may request and issue certificates.

There must be an established process to recover information in the event of lost, compromised or damaged cryptographic keys.

All keys which are used for storing information should be backed up or escrowed. These backup keys should be protected in the same way as the key themselves.

Cryptographic keys that are suspected or confirmed to be compromised must be revoked within an agreed timeframe, as defined by HSC policy.

Owners of cryptographic keys must be aware of and trained on their responsibilities for the protection, usage and disclosure of keys.

Cryptographic private keys must only be disclosed to third parties where obliged by law or regulation and must be approved through local approval processes.

Keys must never be stored on the same system as the information they are used to

encrypt/decrypt.

Encryption keys, e.g. passwords, must not be communicated within the same channel as the encrypted data, for example, a password must not be sent within the same email as the encrypted data, or a USB stick must not be packaged and shipped together with its password. See Information Security Data Transfer Standard (Appendix 7) for more information.

Archived keys must be stored separately from active keys.

Measures must be in place to protect the confidentiality, integrity and availability of archived keys.

When a staff member with knowledge of a secret or private key leaves the organisation, or is no longer permitted access to information protected by the key, the keys must be changed (and all encrypted information must be re-encrypted with new keys if necessary).

When a cryptographic key expires or is no longer required, it must be de- registered and all copies of the key must be securely and verifiably destroyed.

Cryptographic keys must be destroyed in such a way that ensures they cannot be recovered by either physical or electronic means.

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.

APPENDIX 9

1.09 Incident Identification and Reporting All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

An information security incident is a breach of one or more of our information security controls that puts HSC information at risk. No two incidents are the same and, depending on the circumstances, a different response will be needed – however, with prior planning, practice and the right resources in place, negative incident outcomes can be reduced.

Identifying, managing and reporting information security incidents effectively is important in order to comply with legal regulations, to protect the reputation of HSC organisations and to ensure the confidentiality of our staff, clients and patients.

PURPOSE

The purpose of this standard is to ensure a consistent and effective approach to identifying and managing information security incidents. It establishes requirements for response planning, identification of an incident using logging and monitoring of security events, incident response actions, and capturing forensic evidence.

SCOPE

This 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, including:
    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - 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.

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.

INCIDENT IDENTIFICATION AND REPORTING

Security Incident Response Plan

There must be a local and regional cyber-security response plan, and a set of procedures that enable all applicable teams to work in a coordinated way to manage the incident and recover effectively. An effective incident response plan must include the following information:

- Structure of the incident response capability, including key contacts;
- Incident classifications that relate to the risk appetite of the organisation;
- Escalation criteria and processes;
- Available conference number for urgent incident calls;
- Description of the incident life-cycle process (including containing, analysing, remediating and recovering from an incident);
- Guidance on regulatory requirements;
- Procedures that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified security incidents should be reported in a timely manner;
- Playbooks for specific incident types (e.g. ransomware attack, data breach); and
- Links to disaster recovery, business continuity and communication plans.

The incident response plan and procedures must be maintained and regularly updated to ensure that the HSC organisation can effectively prepare, detect, analyse, contain, eradicate and recovery from security incidents.

The incident response plan and procedures must be regularly tested and/or exercised to determine the incident response effectiveness.

The incident response plan must be protected from unauthorised disclosure or modification.

An incident report must be maintained and updated throughout the incident response life-cycle.

Resourcing and Training

HSC organisations must have a defined Cyber Security Incident Response Team (CSIRT), with a central point of co-ordination.

Core roles must be assigned and documented for the CSIRT in order to ensure that incidents are managed and coordinated effectively. As a guide, these should fall under the headings:

- Government and law enforcement;
- Senior / Executive management;
- Incident manager;
- Technical lead / recovery manager;
- Crisis management, business continuity, disaster recovery;
- Investigators and analysts, cyber security specialists;
- ICT and infrastructure; and
- Other departments including legal, PR, HR.

HSC organisations must implement an incident handling capability for security incidents that is scalable, dynamic and commensurate with the level of risk posed.

HSC organisations must provide regular incident response training to staff consistent with assigned roles and responsibilities.

Where it is required for their official duties, staff must receive training for producing evidence and event logs.

Security Event Logging

Event logging must be enabled to record user activity (regardless of account privileges), exceptions, faults and information security events. These records must be held in the relevant regional Security Incident and Event Management (SIEM) system.

Security related events must be logged, stored in approved SIEM storage locations and protected against unauthorised access, modification or deletion, and in conjunction with the regional SIEM capability.

Information systems must have enough capacity to generate the required event logs.

Security related events must be retained, in conjunction with the regional SIEM capability, to enable forensic investigation while adhering to local legislation and regulations.

Administrator and operator logs must include the recording of 'non-human' or system account activity.

ICT system clocks must be synchronised to a universal time source to ensure events can be correlated within an accurate and consistent timeline.

Security Event Monitoring

Application, information system and network logs must be monitored continuously, in conjunction with the regional SIEM capability, and reviewed to detect unusual behaviour. Unusual behaviour includes, but is not limited to:

- Privilege escalation;
- Accessing files that are not required for the staff member's role;
- Downloading more files than is typical for the staff member;
- A large volume of emails being sent from a staff member's account;
- A large volume of emails being sent to staff accounts from an external email address; and
- Sending files outside of the organisation.

Any unusual behaviour identified must be reported to the BSO ITS service desk.

Cyber-Security Incidents

Cyber-security incidents must be identified and subsequently reported to the BSO ITS service desk and information governance officer as quickly as possible:

- When security controls are breached;
- In case of a failure of a security measure that detrimentally affects or attempts to affect the confidentiality, integrity and/or availability of HSC information or systems; or

- When unusual behaviour is detected through protective monitoring; and
- Non-compliance with policies, standards and guidelines.

All staff must report any actual or suspected security incident as soon as they are aware of it and do so in line with local reporting processes.

All staff must report any actual or suspected security incident of lost HSC hardware as soon as they are aware of it and do so in line with local reporting processes.

All staff shall exercise discretion and not externally disclose information about any information security incident, unless required to do so as part of official duties (e.g. to meet regulatory or legal responsibilities, to inform law enforcement, or another relevant authority).

Information Security incidents must be classified in accordance with pre-defined criteria (e.g. critical, high, medium, low) within the regional cyber security incident response plan.

Local, regional and major cyber security incidents must be categorised in accordance with pre-defined criteria (e.g. malicious code, data breach, phishing).

The classification and categorisation of a security incident shall drive the appropriate response to the incident and its priority.

The identification, classification, categorisation and response of potential and confirmed security incidents must be tracked and documented in line with the cyber-security incident response plan.

Forensic Evidence

Any evidence should be collected as soon as possible after the incident. Where forensic collection is performed manually, or a tool is configured to conduct the collection automatically, it must be completed by a competent individual(s).

HSC organisations must maintain a capability to perform enterprise and endpoint forensics in order to support cyber-incident response processes, identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

A process must be established to deal with ICT security incidents or other events that require forensic investigation that includes;

- How evidence is identified;
- How evidence is collected;

- How evidence is acquired; and
- How evidence is preserved.

Evidence shall be collected in adherence with the following:

- To a standard in line with the intention of possible legal action;
- With respect for individuals' privacy and human rights;
- From ICT sources relevant to the incident (e.g. email usage, memory caches, event logs);
- From non-ICT sources relevant to the incident (e.g. CCTV recordings, eye witness accounts); and
- Integrity of the evidence is protected.

Post-Incident Management

The HSC Organisation must document knowledge gained from analysing and resolving security incidents. This document, if required, must be reported to appropriate risk and governance boards, and the cyber programme board, in order to extract lessons learned, and initiate activity to reduce the likelihood or impact of a reoccurrence of similar incident in the future.

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.

APPENDIX 10

1.10 Remote and Mobile Working All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

HSC provide a remote working capability to support the efficient delivery of HSC operations away from a HSC Organisation's site. Staff therefore have access to sensitive data, networks and valuable HSC resources away from the information security controls typically provided by a HSC environment. It is therefore important to understand and take precautions to minimise the potential risks faced to the security of HSC information assets and systems.

PURPOSE

This Standard sets out the need for a safe and secure working environment with appropriate controls in place to protect against a wide range of threats (including theft, terrorism or espionage). This Standard is designed to ensure all users are aware of the risks and their responsibilities when working remotely in order to minimise the potential risk of an information security incident occurring.

SCOPE

This Information Security Standard applies to:

- HSC or NIFRS devices only.
- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS, including:
    - Health and Social Care (HSC) employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - 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.

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 (Appendix 9).

REMOTE AND MOBILE WORKING

Access Control

All staff must ensure they pay due care and attention to avoid unauthorised access to remote and mobile devices.

Remote devices should be used for HSC business use only.

Staff must be granted permission for remote working by the local approval mechanism.

Staff must get BSO ITS approval for hardware and software that can be used remotely. The equipment and software must only be procured and installed by the local IT department.

An information security risk management process must be established to ensure that information security controls maintain risks within acceptable levels.

Remote devices should securely connect to the HSC network through encrypted channels as referred to in the Information Security Encryption Standard (Appendix 8).

Identification and authentication must take place before individuals can remotely access organisation computing facilities.

All login details and passwords to devices connecting remotely should follow the Information Security Accounts and Passwords Standard (Appendix 11).

Equipment usage and sharing must be line with local policies.

All staff must minimise the amount of information stored on a remote device to only that which is needed to fulfil the HSC business activity.

Use of Remote Computing Facilities

Staff must not change the configuration of any HSC remote computing device, install or update any software or hardware of any computing equipment, unless authorised by BSO ITS.

All staff must ensure that remote devices are regularly connected to the HSC network in line with local policy (e.g. once a week) to enable security updates to take place.

All staff connected to HSC networks using personally owned computing equipment must use up-to date anti-malware software.

All HSC equipment must be switched off, logged off, or screen locked when not in use or unattended.

Staff must not send, via any means, personal identifiable or business sensitive information to their personal email accounts.

Staff should refrain from storing files locally (on the devices own drive or desktop), particular if they contain personal identifiable or business sensitive information.

Staff should not take screenshots or photographs of personally identifiable or business sensitive information.

All devices that have been used to store HSC information should be subjected to a secure removal of information process when the device is no longer required, or it is lost/stolen, via the local IT department.

All staff leaving the organisation or no longer requiring use of remote working facilities must return devices to their line manager and/or the IT Department. Please see the appropriate local policy.

Physical and Environmental Control

All staff must pay due care and attention when working remotely to guard against the theft, loss and unauthorised access to remote computing facilities or sensitive data.

All staff must ensure that the work environment outside of the organisational premises offers a suitable level of privacy (e.g. non-staff not being able to see papers, screens or hear confidential conversations).

All staff must take care to avoid the risk of inappropriate display of portable and remote computer and device screens in public places.

All staff must store remote computing facilities and paper documents in approved and locked furniture (e.g. secure filing cabinets) when not in use. Devices must not be left unattended in cars unless absolutely necessary, and never for extended periods of time. If a device has to be left in a car for a short period of time then it must be stored out of view (e.g. in the boot of the car).

All staff should only use trusted and genuine public or free Wi-Fi services. Devices must be logged off the network after use.

Sensitive documents must be collected from remote printing facilities as soon as they are produced.

Sensitive documents must not be taken away from HSC premises unless prior approval is granted within the appropriate local policy.

Documents containing sensitive information must be disposed of in accordance with the Records Management policy.

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 and local policies and procedures

HSC may at any time, and without notice, request a software and hardware audit, and may remove any remote computing facilities at the time of the audit for further inspection. All users must co-operate fully with any such audit.

A regular review of remote access accounts will be carried out. Accounts which are no longer used will be closed.

APPENDIX 11

1.11 Accounts and Password All User Standard

INTRODUCTION

HSC Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

Users are an important part of information security and the controls that authorise, and manager user access requires their identity to be known and trusted. Accounts and passwords provide this important line of defence that protects HSC against unauthorised access to our digital information assets and systems.

PURPOSE

The purpose of this standard is to establish consistent creation, use and termination of user accounts across HSC and NIFRS, and also to ensure that strong authentication practices are used to ensure that only authorised access to the accounts takes place.

SCOPE

This 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, including:
  - HSC and NIFRS employees;
  - Temporary Staff including agency and students;
  - Voluntary Health Sector organisations / Volunteers;
  - 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.

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 (Appendix 9).

ACCOUNTS AND PASSWORDS

Shared Accounts

Shared / Generic accounts are not encouraged, however where it is the only option available for a specific operational purpose, its use must be in accordance with local procedures, used only for the intended purpose, monitored for unauthorised access, and secured with a password that complies with this Standard.

User Requirements

New Accounts and Access Privileges

If a user requires an account (e.g. they are joining an HSC organisation), or they require an additional access privilege (e.g. they have taken on a role that requires access to a restricted storage location), their line manager is required to request the account or access privileges, as necessary and following local procedures, on behalf of the user.

All new user accounts (e.g. for new staff) will be provided with a unique username and temporary password. It is the responsibility of staff to immediately change their default password(s) upon first use, and to meet the minimum requirements outlined within this standard.

Transferring and Changing Accounts and Access Privileges

If a user is changing roles, and that change requires alternative accounts or access privileges, line managers – both current and future - are required to request revocation or access, as necessary and following local procedures, on behalf of the user.

If a user requires a change to their access privileges, their line manager is required to request revocation or access, as necessary and following local procedures, on behalf of the user.

Removal of an Account or Access Privileges

If a user no longer requires an account (e.g. they are leaving an HSC organisation), or they no longer require an additional access privilege (e.g. they have finished working on a project that required access to a restricted storage location), the line manager is required to request revocation, as necessary and following local procedures, on behalf of the user.

User Passwords

Passwords are the first line of protection for user accounts and therefore their strength is key in the organisation's defence against security breaches. All staff are accountable for safeguarding their authentication information.

Password Protection

In order to reduce the risk of compromise, all passwords are to be treated as commercially sensitive information.

All staff must ensure HSC passwords are:

- Not disclosed or shared with anyone, including supervisors, co-workers and the ICT Service Desk;
- Unique for each of their work-related accounts;
- Not re-used for or from their own personal accounts;
- Not transmitted in electronic form over a network including, but not limited to, email or phone;
- Not stored in clear text (e.g. password spreadsheet); and
- Reset on suspicion of compromise by informing your local ICT department. See Information Security Incident Identification and Reporting Standard for more details.

All staff must ensure that accidental disclosure does not take place when entering authentication information, or any other sensitive data, (e.g. typing a password that is visible on screen, when using the keyboard or a virtual keyboard - such as that on an office printer or tablet).

Password Strength

Passwords shall be at least 8 characters long and must include a mixture of at least three of the following:

- Uppercase characters;
- Lowercase characters;
- Number characters; and
- Special characters.

Best practice guidance provided by the National Cyber Security Centre (NCSC) recommends using three random words together to create a strong, memorable password. For example (minus quotes), *"YellowCoffeeBush"*. To comply with HSC Policy, add numbers and symbols as required to result in a complete and secure password: "*YellowCoffeeBush5!"*

Passwords must not be related to the organisation or system name being accessed (e.g. *"HSCLaptop"*).

Passwords must be hard to guess, avoiding personal information including, but not limited to, names, pets, dates and sports teams.

Passwords must not use letters, numbers or special characters sequentially or in patterns (e.g. "*00000000", "15151515", "ABcdEFgh"*).

Internet Passwords

Service providers on the internet may require staff to register a password in order to gain access. Due to the general insecurity of the Internet, when registering with any Internet services, staff must not use passwords already used for information systems in the HSC organisation.

Staff must not allow internet services to store credentials including passwords to allow automatic logins on shared/multiple-user devices.

Password Change

Staff user passwords shall be changed regularly and in accordance with your local information governance policy.

Staff who have forgotten their password must contact their ICT service support desk, who will issue a replacement providing the employee is able to satisfy all the appropriate security checks as required by local policy.

SYSTEM OWNERS REQUIREMENTS

User accounts and Access Privileges

Accounts and Access Privileges for HSC information systems and network resources require careful oversight. Security precautions should be part of account management to ensure that:

- Only authorised accounts are created;
- The principle of least privilege will be applied for access privileges;
- Only authorised privileged accounts are created;
- Obsolete accounts are disabled in a timely manner; and
- Any access assigned is appropriate to the facilities required by the individual user's HSC business role.

BSO ITS are responsible for carrying out and documenting an audit of all operational accounts, ensuring that each account is owned by a member of staff still employed in the organisation and that the associated account privileges are appropriate to their job function. This audit should be actioned on a monthly basis.

New Users

Access to HSC information systems shall be controlled through a formal user registration process beginning with a formal request to BSO ITS. All line managers must authorise the level of access required for a role.

Each staff member must be provided with a unique username and temporary password.

Temporary passwords must comply with the minimum password requirements documented in this standard.

Staff are not permitted to authorise or action the creation of accounts or set access privileges for their own use.

Change of User Requirement

Staff that request a change to their requirements, e.g. a small adjustment of applications or access must be approved, and submitted where required by local policy, by their line manager and BSO ITS must be notified.

If the change relates to a user moving to a different role or requiring a different level of access, the previous line manager must initiate the change of access request to

remove the current levels of access. The line manager for the new role will need to initiate a change of access request for the new levels of access required.
Line Managers must not pass usernames and passwords from one post-holder to another.

Removal of Users

When a member of staff leaves the organisation or no longer requires use of an account:

- Line managers must inform BSO ITS of the removal of the account and provide them with all associated user privileges.
- The local ICT department must ensure access rights to all information systems are revoked immediately.
- An audit must be kept of the removal of all user requests on local record management systems, outlining when they were requested, reviewed and removed.

Privileged Accounts

A privileged account is an account that has more privileges than ordinary users, such as service or system accounts that may have administrator capabilities, or carrying the permission to make changes to system configuration. BSO ITS must ensure when a regional privileged access management (PAM) solution is in place that:

- The allocation of a privileged account is restricted to predefined purposes based on HSC business needs;
- Privileged accounts are linked to an identifiable (i.e. unique) owner;
- Privileged accounts are only granted on the basis of a formal, authorised access request that specifies the required privileges;
- The maximum age of a privileged account password must be in line with the requirements of any applicable regional privilege management policy.
- Local privileged account sessions must log off in line with the requirements of any applicable regional privilege management policy;
- Privileged accounts must only be used for the official duty that requires such access and not used for regular HSC business activities that could be carried out with a non-privileged account such as accessing email or browsing the internet;
- Privileged accounts must have a different password to a standard account;
- All activities performed using privileged accounts are logged, and reviewed periodically and independently; and

- Any changes to privileged accounts are logged, and reviewed periodically and independently.

Temporary Users

When it is necessary to set up temporary access to information systems for the use of agency staff, consultants or other visitors, a temporary account must be created with the appropriate restricted privileges and settings in line with local Access Management and Third-Party Management policies.

BSO ITS must:

- Ensure that an audit of all activities performed from the account is kept;
- Ensure that the temporary user account is disabled upon the completion of work or termination of the contract etc;
- Ensure that an audit is kept of account privilege and password creation and any amendments made to them; and
- Retain records in order to provide evidence of compliance with this standard.

Remote access by third parties to the organisation's information systems may be required, in such circumstances refer to local Third-Party Management and Remote and Mobile Working policies for guidance.

Passwords

System owners should only design the use of passwords into their system where they are absolutely necessary and appropriate. Other authentication mechanisms, such as single sign-on (SSO), hardware tokens and biometrics, must be considered for security and user experience benefits.

Multi-factor authentication (MFA) shall be used when a regional PAM solution is in place for all privileged access systems, services, data and internet facing systems.

System owners (BSO ITS) must implement the following technical solutions where available:

- Throttle or use account lockout, allowing 5 login attempts before locking out;
- Monitor for malicious or abnormal behaviour such as brute for attacks, login attempts from unexpected locations or login attempts that fail the second step of MFA;
- Blacklist common or easily guessable passwords from being used;
- Users can select and change their own passwords and include a confirmation

procedure to allow for input errors;

- Where applicable, enforce HSC users to change their temporary (new account) passwords at the first log-on;
- Prevent re-use of the previous 5 passwords;
- Do not automatically display passwords on the screen when being entered;
- Prevent passwords shorter than 8 characters; and
- Do not use artificial capping on password length.

HSC organisation's web applications requiring authentication must use HTTPS.

Passwords must not be stored in plain text and where possible should be stored in hashed format using multiple iterations of the hash function. Applications must add a 'salt' to a password before hashing. The hash functions must follow industry encryption standards (such as PBKDF2), for example SHA-256.

Any default vendor supplied passwords that come with any system, software or device must be changed before deployment.

User guidance or awareness programmes on passwords must focus on improving security such as:

- The risks of re-using passwords across work and home accounts;
- How to choose passwords difficult to guess;
- How to avoid reusing passwords; and
- Encouraging reporting when something is suspicious.

Passwords must not be shared, rather HSC should use alternative solutions to support the HSC business need for sharing accounts.

Delegation must be used in preference to sharing accounts (such as delegated access to a storage repository, digital document or inbox).

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.

APPENDIX 12

Information Security frameworks, legislation, regulation and guidance:

- **Computer Misuse Act (1990)** Covering unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences, unauthorised acts, causing or creating risk of serious damage to computer systems.
- **General Data Protection Regulation (GDPR)** Specifically **chapter 2, chapter 4, chapter 5** and the fundamental principles as listed below:
    - Lawful, fair and transparent
    - Purpose limitation
    - Data minimisation
    - Accuracy
    - Storage Limitation
    - Integrity and Confidentiality
    - Accountability
- **Data Protection Act 2018** Specifically **chapter 4** and covers a number of offences in relation to the control and access of data specifically **section 55, section 170** and the fundamental information principles as listed below:
    - Must be used in a way that is adequate, relevant and limited to only what is necessary
    - Must be handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- **Network and Information Systems 2018** The goal of the Network and Information Systems Regulations of 2018 (NIS Regulations) is to drive improvement in the protection of the network and information systems which are critical for the delivery of digital services and essential services in the UK.
- **HMG Civil Contingencies Act 2004** How the government prepares and plans for emergencies, working nationally, locally and co-operatively to ensure civil protection in the UK.
- **The Copyright, Designs and Patents Act 1988** The Copyright Designs and Patents Act (1988) gives creators of digital media the rights to control how their work is used and distributed.

- **The Access to Health Records Act 1990** and **Northern Ireland Order (1993)** The Access to Health Records Act 1990 allows patient's personal representatives and any person who may have a claim arising out of the patient's death access to their record. The Northern Ireland Order (1993) has been repealed to the extent that it now only affects the access to health records of deceased patients.
- **The Health and Safety at Work (NI) Order (1978) Health and Safety (display Screen Equipment) Regs (NI) 1992** The Order imposes duties on employers to look after the health and safety of their employees and responsibilities on employees to comply with the measures put in place for their health and safety.
- The Human Rights Act (1998) Article 8, relating to privacy, is of most relevance to Information Security. It provides a right to respect for an individual's "private and family life, his home and his correspondence".
- **The Employment Practices Data Protection Code** The Employment Practices Data Protection code deals with the impact of data protection laws on the employment relationship. It covers such issues as the obtaining of information about workers, the retention of records, access to records and disclosure of them.
- **The Obscene Publication Act 1958** An Act to amend the law relating to the publication of obscene matter.
- **Freedom of Information Act 2000** The Freedom of Information Act gives individuals a right of access to information held by HSC organisations, subject to a number of exemptions.
- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the Regulations) give businesses the right to monitor communications on their own networks.
- Regulation of Investigatory Powers Act 2000 The Regulation of Investigatory Powers Act 2000 (RIP or RIPA) is an Act of the Parliament of the United Kingdom, regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications.
- **National Institute of Standards and Technology (NIST) Special Publication for Information Security** This Information Security Handbook provides a broad overview of Information Security program elements to assist managers in understanding how to establish and implement an Information Security program. International Organisation for Standardisation (ISO) ISO/IEC 27001 is the best-known standard in the ISO family providing requirements for an Information Security management system (ISMS).
- **ISO/IEC 27001:2013 Information technology** National Cyber Security Centre guidance: Guidance on how organisations can protect themselves in cyberspace, including the 10 steps to cyber security: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

- Cabinet Office - **Security policy framework** (April 2014), **Government Security Classifications** (April 2014).
- DOHNI - **Code of Practice on Protecting the Confidentiality of Service User Information** (April 2019**), Information and Communication Technology Controls Assurance Standards** (2008/9), **DOH & HSC Protocol for Sharing Service User Information for Secondary Purposes** (August 2011)
- NHS Digital HSCN Connection Agreement
- Information Commissioners Office (ICO) **Employment Practices Code Part 3: Monitoring at Work**
- **Protection of Children (Northern Ireland) Order 1978 Protection of Children (Northern Ireland) Order 1978**