Information Security Policy

Approval

Document Reference	Information Security Policy
Version	1.3
Last updated	1st March 2021
Owner	
Approval by	

Contents

1.   INTRODUCTION

Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) (herein HSC will refer to all HSC and NIFRS organisations) Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations. 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 take 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 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 requirements ethically, regulatory and legally applicable to us. To enable this, the objectives set within this Information Security Policy is complimented by two sets of Information Security Standards, for non-technical users and technical users, that should be read for detail into specific areas of Information Security, these areas are as follows:

Standard Reference Number	All User Standards	Standard Reference Number	Technical User Standards
1.01	Email Communications	2.01	Asset Management
1.02	Removeable Media	2.02	Cloud Services and Security
1.03	Use of Internet Services	2.03	Encryption
1.04	Asset Management	2.04	Incident Management
1.05	Clear Desk and Screen	2.05	Remote and Mobile Working
1.06	Cloud Security	2.06	Privileged Account Management
1.07	Data Transfer	2.07	Patch Management
1.08	Encryption	2.08	Vulnerability Management
1.09	Incident Identification and Reporting	2.09	Incident Response
1.10	Remote and Mobile Working	2.10	Network Discovery
1.11	Accounts and Passwords	2.11	Anti-Virus and Endpoint Protection
		2.12	Public Key Infrastructure
		2.13	Wireless
		2.14	Joiners, Movers, Leavers

There are a number of relevant pieces of legislation (see section 9) 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 General Data Protection Regulation (GDPR) define a legal basis for UK organisations to take steps to ensure that personal data is adequately protected by placing a legal obligation on them to do so. HSC are also required to abide by the regulation set out in 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 is appropriate.

2. PURPOSE

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

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

This is to 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

The Information Security Policy applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS [1], including:
    - HSC and NIFRS employees
    - Temporary Staff including agency and students
    - Voluntary Health Sector organisations / Volunteers
    - 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 policy applies throughout the entire information lifecycle from acquisition/creation through utilisation to storage and disposal.

4. MANAGEMENT FRAMEWORK

4.1. STRATEGIC DIRECTION

4.1.1. The Department of Health in Northern Ireland (DoHNI) is responsible for setting

---

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

policy and legislation which directs Information Security Management across the HSC.

4.1.2.   The Health and Social Care Board (HSCB) 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

4.2.1.   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 Regional Director of eHealth and External Collaboration.

4.2.2.   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 DoHNI.

4.3.   CORE INFRASTRUCTURE

4.3.1.   The Business Services Organisation IT Services Unit provides and maintains the central ICT 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 HSCB.

4.4.   COLLABORATION

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

4.5.   OPERATIONAL MANAGEMENT

HSC Cyber Leads Group

4.5.1.   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.

Local Security Management

4.5.2.   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.

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

4.6.   ROLES AND RESPONSIBILITIES

Most Senior Officer (MSO) of each HSC Organisation

4.6.1.   The MSO is responsible to the HSCB for Information Security within their organisation. This is typically the Chief Executive, General Manager or Senior General Practitioner (GP). This role is responsible for:

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

Senior Information Risk Owner (SIRO)

4.6.2.   Responsible to the MSO of their local organisation, e.g. Chief Executive, advising on the information risk aspects of his/her statement on internal controls. Responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- 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 incident management framework.

Data Protection Officer (DPO)

4.6.3.   Reporting to the SIRO, the DPO is an independent Data Protection expert that is accountable for ensuing Data Protection regulations such as the DPA and GDPR are being successfully managed at HSC. The DPO is responsible for:

- Informing and advising HSC's data protection obligations, monitoring internal compliance, and demonstrating compliance where required;
- Providing support and advice to the business 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).

Information Asset Owner (IAO)

4.6.4.   Responsible to the SIRO of their local organisation providing assurance that information risk is being managed effectively in respect of the information assets that they 'own'. 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 information asset and providing assurance to the SIRO.

HSC ICT Security Manager

4.6.5.   Responsible to the BSO ITS Assistant Director, providing assurance that appropriate HSC Information Security policies and procedures, standards and guidelines are in place. 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 ICT Security Managers/Officers, System Managers or others, ensuring the necessary corrective or preventative actions are implemented; and
- Liaising with ICT Security Manager/Officers on matters of Information Security which may impact multiple HSC organisations.

Cyber Lead

4.6.6. Responsible to the SIRO in their organisation providing a local focus on all Information Security matters. Responsible for:

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

System Managers

4.6.7. Responsible to the IAO in their organisation 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 the ICT department to ensure core local processes are consistently applied across all information systems;
- Ensuring users of the systems are appropriately trained; and
- Reporting security matters to the ICT Security Officer/Manager.

Third Party Contractors

4.6.8. 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.

Users of HSC Information Assets and Systems

4.6.9. Responsible for:

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

5. INFORMATION SECURITY POLICY STATEMENTS

5.1. CONTROLS ASSURANCE

5.1.1. 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.

5.1.2. To support and underpin compliance, all HSC organisations shall have:

- Staff who are well trained to exercise good judgement, 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. THIRD PARTY MANAGEMENT

5.2.1. 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.

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

5.2.3. 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.

5.2.4. 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.

5.3. DATA CLASSIFICATION

5.3.1. 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.

5.3.2. 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.

5.4. RECORDS MANAGEMENT

5.4.1. 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.

5.4.2. 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.

5.5. ENCRYPTION

5.5.1. 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 DoHNI.

5.5.2. 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.

5.5.3. See the Information Security 1.08 Encryption Standard for more information. Technical users should see the Information Security 2.03 Encryption Standard and Information Security 2.12 Public Key Infrastructure Standard for more information.

5.6. INFORMATION ASSET AND SYSTEM MANAGEMENT

5.6.1. 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).

5.6.2. 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).

5.6.3. See the Information Security 1.04 Asset Management Standard for more information. For more information, Technical users should see:

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

5.7. DATA PROTECTION

5.7.1. 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.

5.7.2. 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.

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

5.7.4. 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 re-use of an asset or system.

5.8. EMAIL COMMUNICATIONS

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

5.8.2. 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.

5.8.3. See the Information Security 1.01 Email Communications Standard for more information.

5.9. USE OF INTERNET SERVICES

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

5.9.2. 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.

5.9.3. See the Information Security 1.03 Use of Internet Services Standard for more information.

5.10. INFORMATION FLOW CONTROL

5.10.1. 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.

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

5.11. DATA TRANSFER

5.11.1. 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.

5.11.2. 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.

5.11.3. 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.

5.11.4. Where an information asset(s) is being shared or transferred, for example a data set containing personal information is being shared with a third party.

5.11.5. See Information Security 1.07 Data Transfer Standard for more information.

5.12. ACCOUNTS AND PASSWORDS

5.12.1. 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.

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

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

5.12.4. 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.

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

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

5.12.7. See Information Security 1.11 Accounts and Passwords Standard for more information. Technical users should see the Information Security 2.06 Privileged Account Management Standard and Information Security 2.14 Joiners, Movers, Leavers Standard for more information.

5.13. ACCEPTABLE USE

5.13.1. 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.

5.14. REMOTE AND MOBILE WORKING

5.14.1. 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.

5.14.2. 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.

5.14.3. 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.

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

5.14.5. See Information Security 1.10 Remote and Mobile Working Standard for more information. Technical users should see the Information Security 2.05 Remote and Mobile Working Standard for more information.

5.15. MALWARE AND ENDPOINT PROTECTION

5.15.1. 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.

5.15.2. 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.

5.15.3. Technical users should see the Information Security 2.11 Anti-virus and Endpoint Protection Standard for more information.

5.16. EXTERNAL GATEWAYS

5.16.1. 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.

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

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

5.16.4. 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.

5.17. VULNERABILITY/PATCH MANAGEMENT

5.17.1. All HSC organisations must ensure that standards and processes are in place to ensure the patching and vulnerability management of devices and software is in effective at reducing exposure and subsequent risk to known vulnerabilities. This should include at least:

- Roles and responsibilities;
- Response plans and timelines;
- Integration into change management processes;
- Escalation into Incident Response processes;
- Testing processes to ensure compatibility and integrity; and
- Other mitigating controls to take where a fix is not timely or available.

5.17.2. In addition to maintaining a complete inventory of information assets and systems, technical information should be recorded alongside to support the discovery and management of vulnerabilities, for example vendor, version number, and where it is installed.

5.17.3. Technical users should see the Information Security 2.07 Patch Management Standard and Information Security 2.08 Vulnerability Management Standard for more information.

5.18. SECURITY TRAINING AND AWARENESS

5.18.1. 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.

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

5.18.3. 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

5.19.1. All HSC organisations must ensure that standards and processes are in place to support the secure implementation, risk management, and use of cloud services.

5.19.2. Use of cloud services must be agreed with ICT and approved by your local SIRO.

5.19.3. See the Information Security 1.06 Cloud Security Standard for more information. Technical users should see the Information Security 2.02 Cloud Security Standard for more information.

5.20. BUSINESS CONTINUITY

5.20.1. 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 IDENTIFICATION, MANAGEMENT AND REPORTING

5.21.1. 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.

5.21.2. 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.

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

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

5.21.5. See the Information Security 1.09 Incident Identification and Reporting Standard or Regional Incident Response Plan for more information. Technical users should see the Information Security 2.04 Incident Management Standard and Information Security 2.09 Incident Response Standard for more information.

5.22. DATA BACKUP

5.22.1. 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;
  - System configuration and master images.
- The Recovery Time Objective (RTO);
- The Recovery Point Objective (RPO);
- The risk to the information;
- Laws and regulations;

- Security controls;
- Information governance requirements:
  - Retention period
  - Classification and handling procedures

5.23. REMOVABLE MEDIA HANDLING

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

5.23.2. 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; and
- Unknown removable media must not be connected to a 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.

5.23.3. See the Information Security 1.02 Removable Media Standard for more information.

5.24. SECURITY VETTING

5.24.1. 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. TERMS AND CONDITIONS OF EMPLOYMENT

5.25.1. All HSC organisations should ensure that all contracts of employment include statements requiring compliance with HSC and local Information Security policies, standards and procedures. HSC organisations must ensure:

- Contractual obligations are made clear and employees sign terms and conditions;
- Employees are 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 if clearly defined; and
- That access rights are terminated at the end of employment. There are processes for changing or terminating employment.

5.26. PHYSICAL AND ENVIRONMENTAL SECURITY

5.26.1. 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.

5.26.2. 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.

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

5.26.4. Health and Safety legislation must be adhered to at all times and realised in local policies, standards, processes and guidance materials where applicable.

5.27. CLEAR DESK AND SCREEN

5.27.1. 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. locked areas, desks, printers, cupboards, desk drawers, multi-function devices and photocopiers) and computer equipment.

5.27.2. HSC recognises the importance of protecting our information, therefore, all staff must:

- Immediately collect printed media 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; and
- Ensure on-screen or desk content cannot be overseen by unauthorised individuals, especially when in public places (e.g. use display screen protectors).

5.27.3. See the Information Security 1.05 Clear Desk and Screen Standard for more information.

5.28. RISK ANALYSIS AND MANAGEMENT

5.28.1. 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.

5.29. AUDIT AND ACCOUNTABILITY

5.29.1. 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).

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

6. COMPLIANCE (LEGAL/CONTRACTUAL)

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

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

7. REPORTING AN INFORMATION SECURITY INCIDENT

7.1.1. Information Security incidents must be identified and subsequently reported to the local 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

7.1.2. See the Information Security 1.09 Incident Identification and Reporting Standard for more details.

8. NON-COMPLIANCE / POLICY BREACHES

8.1. SANCTIONS

Failure of HSC Organisations

8.1.1. 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 internal ICT management framework group.

8.1.2. 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 at HSCB level will be taken by the Regional Director of eHealth and External Collaboration.

8.1.3. 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.

Failure of HSC Employees

8.1.4. 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.

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

8.1.5.   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

9.1.1.   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.

9.1.2.   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

10.1.   MINIMUM LOCAL POLICIES / PROCEDURES

10.1.1. 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 and Technical Information Security Standards as listed in Section 1 of this policy.

10.1.2. Legislation imposes a need for all HSC organisations to take steps to ensure compliance with all statutory requirements. The following Information Security frameworks, legislation, regulation and guidance have been used to underpin the development of this policy - note this list is not exhaustive:

Source	Comment
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

11. PROCEDURES TO IMPLEMENT THE INFORMATION SECURITY POLICY

Standard Reference Number	All User Standards	Standard Reference Number	Technical User Standards
1.01	Email Communications	2.01	Asset Management
1.02	Removeable Media	2.02	Cloud Services and Security
1.03	Use of Internet Services	2.03	Encryption
1.04	Asset Management	2.04	Incident Management
1.05	Clear Desk and Screen	2.05	Remote and Mobile Working
1.06	Cloud Security	2.06	Privileged Account Management
1.07	Data Transfer	2.07	Patch Management
1.08	Encryption	2.08	Vulnerability Management
1.09	Incident Identification and Reporting	2.09	Incident Response
1.10	Remote and Mobile Working	2.10	Network Discovery
1.11	Accounts and Passwords	2.11	Anti-Virus and Endpoint Protection
		2.12	Public Key Infrastructure
		2.13	Wireless
		2.14	Joiners, Movers, Leavers

12. REVIEW CYCLE

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

12.1.2. All HSC organisations are responsible for ensuring their own local policies, standards and procedures are subject to regular review and take into account any

changes to this Information Security Policy.

<<Add Name>>.

<<Add Role>>   Date: 19/02/2020

<<Add Name>>.

<<Add Role>>   Date: 19/02/2020