HSC Supplier Security Policy

Approval

Document Reference	HSC Supplier Security Policy
Version	0.15
Last updated	05 April 2022
Owner	HSC Cyber Programme
Approval by	

Contents

1. DEFINITIONS

“Third Party” means any business partner, supplier, contractor, sub-contractor, reseller, distributor, joint venture, consortium, teaming partner, law firm or other business partner that will assist HSC in delivering services.

“HSC Information System” means any information system owned or controlled by HSC and used to store, process, transmit, or receive HSC Information. It also means any patient information systems or acquired services to the extent such information systems or services are physically or logically connected to HSC Information Systems or owned, controlled, managed or supervised by HSC organisations. Including the associated operating systems, applications and databases, either open-source or vendor provided.

2. INTRODUCTION

In entrusting its information and assets to external third parties HSC requires assurance that their integrity is maintained at every point in the supply chain, and those requirements are defined in the HMG Security Policy Framework (SPF). In addition there are also legal compliance requirements defined in the Data Protection Act 2018 (GDPR).

This policy document and the standards from which it is derived addresses the security assurance requirements in the contract management lifecycle. It applies to, and is intended for use by all HSC bodies, Northern Ireland Fire and Rescue Service (NIFRS) and their contracted staff (third party suppliers) engaged in supporting HSC and NIFRS services.

The requirements set out in this document are intended to support everyone involved in secure delivery of contractual obligations. In meeting these requirements it will assist HSC in achieving and maintaining ISO 27001 certification by mandating the information security controls required to meet Section A.15 of that standard. Effective information security is achieved by implementing a suitable set of controls to ensure that the specific security objectives of HSC are met. The data and information that HSC information systems contain, with particular regard to patient and client based data, must only be seen by those who are entitled to see it on a “Need to know basis”.

Health and Social Care in Northern Ireland are provided as an integrated service. There are a number of organisations who work together to plan, deliver and monitor Health and Social care across Northern Ireland.

3. PURPOSE

This policy sets out the requirements expected of third parties in order to effectively protect HSC information. This policy will ensure that HSC complies with its statutory duties laid out in the Data Protection Act 2018.

It will ensure that all third party organisations who enter into an agreement or contract with the HSC organisations are clear about the requirements in terms of information security and confidentiality.

It will ensure that all parties acting as a data processor for HSC will have the relevant technical and security measures in place to meet data protection legislation and privacy requirements.

The correct application of this policy will ensure that HSC is compliant with its legislative responsibilities, reduce the risk of an information security breach taking place and provide assurance to our staff and patients that information assets are being properly managed.

4. SCOPE

The scope of this policy is any third party which will process or have access to any HSC Information or information systems. This includes, but is not limited to:

- Third Party suppliers involved in the design, development and/or operation of information systems for any HSC organisation, writing and installing bespoke software, contractual support arrangements or operation of systems.
- Access to HSC information from remote locations where the computer and network facilities are not under the control of HSC
- Third parties who are not employees of any HSC organisation and require access to HSC information or information systems
- Access to HSC information via non-HSC applications and systems, which are hosted external to the HSC Network.

5. SECURITY ASSURANCE FOR THIRD PARTIES

A standardised process and framework for managing ICT contracts is used by HSC. Disclosure of HSC Information to third parties or access to HSC Information Systems shall not take place unless adherence to the HSC Cyber Security Assurance Framework is evidenced by third parties.

New ICT Contracts to HSC

New ICT contracts will be risk assessed using the HSC Cyber Supplier Risk Assessment Questionnaire (see APPENDIX B – REFERENCES). This will take place pre-procurement. The Service will return the completed questionnaire to the HSC body carrying out the compliance piece. This response will then be scored to determine one of four different Risk Profiles for the contract, each Risk Profile having a corresponding set of ICT security requirements.

Included in these requirements are a security accreditation requirement, where the chosen third party will self-certify that they have (or can commit to obtain, prior to the commencement of the contract) ICT Security certification that covers the scope required for all aspects of the contract, and that they commit to maintaining this standard for the duration of the contract. Third parties will also be expected to adhere to an HSC Security Management Schedule, this HSC Supplier Security Policy, and the HSC Network Code of Connection.

In addition, third parties may be subject to a "right to audit" clause by the procuring organisation, as set out in contract, and will fully cooperate with any audits or investigations.

Depending on the risk level associated with the contract, a request for evidence of any IT Health Checks carried out in the previous 12 months; or an IT Health Check performed by a CHECK Service Provider and/or an onsite security audit undertaken by the procuring organisation or their designated representative, may be made.

Risk Profiles

N/A – Requires no additional ICT security requirements beyond the standard T&Cs of the contract.

LOW – Cyber Essentials (self-certified) certification, HSC Security Management Schedule (Low and Medium Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection.

MEDIUM – Cyber Essentials Plus certification, HSC Security Management Schedule (Low and Medium Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection. Evidence of an IT Health Check carried out in the previous 12 months.

HIGH – Cyber Essentials Plus or ISO 27001 certification, HSC Security Management Schedule (High Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection. An IT Health Check performed by a CHECK Service Provider, at the behest of the procuring organisation.

Security Assurance Review Outcome

All relevant information security requirements shall be established and agreed upon with each third party that will access, process, store, or communicate HSC Information, or provide HSC with IT infrastructure components that process HSC information. Legacy contracts that have been assessed as high risk by HSC Security, are to be brought into compliance with this standard upon renewal. All other legacy contracts are to be brought into compliance with this standard on a commercially reasonable effort.

6. SUPPLY CHAIN SECURITY MANAGEMENT

To maintain the confidentiality, availability, and integrity of HSC Information Systems, security requirements in service agreements with third party suppliers that deliver services or products to HSC and access HSC Information Systems as part of the delivery, shall be implemented.

Prior to their engagement, third parties may be subject to an independent, risk based due diligence evaluation. Information security requirements to mitigate the risks associated with a third party's access to HSC Information and Information Systems shall be agreed upon and documented as part of the final third party contractual agreement covering provision of third party's products and services.

7. RESPONSIBILITIES

Third parties providing products and services must confirm their compliance with the baseline security standards and obligations outlined in this security policy, to ensure appropriate measures have been taken and are in place to assure the continued security of the product or service provided.

The HSC supply chain and partners that we share data with have a responsibility to provide appropriate and continued protection for the full life span of any information shared. This extends to any further authorised sharing undertaken with another party with whom the Supplier enters into a Sub-contract. Third parties and partners are responsible for ensuring HSC requirements are passed down to those parties.

8. DATA PROTECTION AND PRIVACY

The third party organisation shall ensure compliance with all applicable laws and regulations relating to the processing of data and privacy protections. The current UK legal requirement for the lawful and correct handling of personal data is set out in the Data Protection Act 2018. This Act makes provision for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information. Third parties shall comply with the requirements of this legislation at all times. Any non-compliance shall be notified in accordance with the HSC incident management process.

The third party shall ensure accuracy and completeness of controls to ensure the integrity of the information or information processing provided.

9. DATA CLASSIFICATION

HSC information is classified in terms of its value, legal requirements, sensitivity and criticality to the organisation. Each HSC organisation's Data Classification Policy contains direction on:

- 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

10. DATA PROCESSING AGREEMENTS

The HSC Data Access Agreement Template can be found in Appendix B.

11. CALDICOTT PRINCIPLES

The following principles, drawn from the Caldicott Report 2013, must be upheld in respect of the holding and passing on of patient or client information to organisations within and outside the HSC.

1. Justify the purpose(s) for using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict need-to-know basis.
5. Everyone must understand his or her responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality

12. DATA PRIVACY IMPACT ASSESSMENTS

If personal data will be involved, a Data Privacy Impact Assessment must be undertaken by the Service, in conjunction with the third party, to understand the risk to the HSC data and to ensure GDPR is complied with. Guidance on DPIAs can be found here.

13. THIRD PARTY SYSTEMS SUPPORTING HSC

Development, test, and production facilities processing HSC Information must be separated to reduce risks of unwanted changes or unauthorised access to live HSC data. Live patient Information must not be used in development or test facilities.

14. THIRD PARTY ROLES AND RESPONSIBILITIES

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unintentional or unauthorised modification or misuse of HSC information.

15. THIRD PARTY PERSONNEL SECURITY

Security Screening, Confidentiality agreements and the prevention of terminated employees from accessing HSC Information and disciplinary measures for employees who violate information security policies and standards shall be in place.

15.1. SECURITY TRAINING

All Supplier Staff that have the ability to access HSC Information or Information Systems shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority / HSC in writing, this training must be undertaken annually.

15.2. THIRD PARTY MOVERS AND LEAVERS

HSC shall be informed immediately when a third party employee or sub-contractor with any HSC account is terminated from their employment or no longer supports HSC.

16. INFORMATION SECURITY MANAGEMENT SYSTEM

Operating procedures for information security management and controls related to HSC Information must be documented, maintained and made available to users involved in accessing or processing HSC Information and systems.

17. DEFINITION OF A SECURITY INCIDENT

The NCSC defines a cyber-incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

1. Attempts to gain unauthorised access to a system and/or to data.
2. The unauthorised use of systems for the processing or storing of data.
3. Changes to a systems firmware, software or hardware without the system owners consent.
4. Malicious disruption and/or denial of service.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

All third party 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.

19. CHANGE CONTROL FOR THIRD PARTY SERVICES

Changes to the provision of services by third parties, including maintaining and improving existing information security policies, procedures and controls, shall be managed, based on the criticality of business information, systems, and processes involved and re-assessing risks. HSC must be informed in advance of any proposed changes that could impact the CIA of HSC data or information systems. All changes will be subject to a security assessment, which may require an amendment to the contract.

20. SUB-CONTRACTING OF SERVICES

A Sub-contractor is any third party with whom:

(a) The Supplier enters into a sub-contract; or

(b) A third party under (a) above enters into a sub-contract, or the servants or agents of that third party.

21. CLOUD COMPUTING

Only shared hosting or As A Service (aaS) services that have been subject to an independent, risk based due diligence evaluation in accordance with the HSC Cloud Security Policy shall be used. HSC Information shall not be shared or stored with a hosting or aaS third party unless the security controls required by the contract or agreement are in place.

Before HSC Information is transferred for storage or processing to a shared hosting or aaS third party, the Supplier shall provide evidence that they protect the hosted environment and HSC Information as required by the contract or agreement and commensurate with the security categorisation of the HSC Information, as required by the HSC Cloud Security Policy.

22. COMPLIANCE

Any Supplier who violates this policy may be disabled from continued use/access to HSC, until a full investigation is complete.

APPENDIX A – LIST OF ORGANISATIONS

Strategic Planning and Performance Group (SPPG)

Public Health Agency (PHA)

Northern Health and Social Care Trust (NHSCT)

Southern Health and Social Care Trust (SHSCT)

South Eastern Health and Social Care Trust (SEHSCT)

Western Health and Social Care Trust (WHSCT)

Belfast Health and Social Care Trust (BHSCT)

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

NI Fire & Rescue Service (NIFRS)

And other Independent Contractors to HSC.

APPENDIX B - REFERENCES

Reference	Title	Location
Ref A	HSC Information Security Policy	 HSC Information Security Policy
Ref B	HSC Network Code of Connection	 HSC Network Code of Connection
Ref C	HSC Data Access Agreement	 Data Access Agreement (v4.0)
Ref D	Secure Remote Access Form	 Secure Remote Access Form
Ref E	Statement of Compliance Form for Third Parties	 Compliance for Third Parties
Ref F	HSC Cyber Supplier Risk Assessment Questionnaire	 HSC Cyber Supplier RAQ