NIPEC/16/15

NIPEC

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

ICT Security Policy

July 2016

Review Date: June 2019

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

www.nipec.hscni.net

TABLE OF CONTENTS

1 Introduction

Data and Information stored within the many Health and Social Care (HSC) information systems represents HSC's most valuable asset so there is a need to develop an environment within which information systems and networks can be secure.

The Data Protection Act (1998) defines 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.

This security of information can be achieved through technical means but it is limited and should be supported by appropriate management and procedures. Insider threat is still the biggest threat whether this is intentional or accidental. Effective information and ICT security management requires the participation of, all employees and council members, hereafter referred to as the 'users' in the organisation.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls should be established to ensure that the specific security objectives of the HSC are met and that the data / information HSC information systems contain, with particular regard to patient and client based data, is seen only by those entitled to see it.

Within NIPEC, staff, hardware, software, telecommunications, facilities and data together form an IT system that is highly effective and productive. However, all IT systems involve certain risks that must be addressed adequately through proper controls. The practices and procedures contained in this document represent the organisation's commitment to assuring confidentiality, integrity, availability and control of NIPEC's IT resources.

Within NIPEC, it is essential for each user on the network to recognise their responsibility in having access to vast services, sites, systems and people. The user is ultimately responsible for their actions in accessing network services.

Within the Internet users may find themselves within other networks (and/or the computer systems attached to those networks). Each network or system has its own set of policies and procedures. Actions, which are routinely allowed on one network/system may be controlled, or even forbidden, on other networks. It is the users responsibility to abide by the policies and procedures of these other networks/systems. Remember, the fact that a user **can** perform a particular action does not imply that they **should** take that action. The use of the network is a privilege, not a right, which may temporarily be revoked at any time for abusive conduct.

The practices and procedures contained in this document are applicable to all IT resources at all levels within the organisation, whether maintained in-house or managed externally. These practices and procedures are mandatory on all staff, and others having access to and/or using the IT resources of NIPEC. The contents applies to all automated technologies currently in existence and to any new automated technology acquired after the effective date of this policy document.

1.1 NIPEC

1.1.1 The Environment

NIPEC's IT system, which is managed through a Service level Agreement (SLA) with the Business Services Organisation (BSO) operates on a Cat 5 RJ45 cable environment, which links each desktop machine to the main NIPEC information server (accessible via the N Drive), that is located in BSO ITS, Centre House. Within the organisation, there is a common PC Platform using a common operating system of Window 7 Enterprise. This information server, also serves as a Blackberry Server which carries out all operations relating to the handheld Blackberry Leap handheld devices currently providing access to emails and internet to 9 members of staff within the organisation.

Each machine links to the NIPEC Server (N Drive), via network points located within each office. These points are managed by two Cisco C3kx NM10 Switches, which are located within the Computer Storage Room.

Whilst using the network, staff may make use of a number of shared resources, e.g. the Xerox Multi-Devices, as well as files and folders (provided the staff member has the appropriate security permission).

The NIPEC Server is explained in more detail below: -

NIPEC Server
This server contains all the Email mailboxes (accounts and messages), allows Internet access from each desktop within the organisation, the Internal Filing Structure (which mirrors the structure of Central registry). Each member user has a small area (folder) on the server to store items that is backed-up on a nightly basis. Access to these folders is restricted to the specific user, and the BSO, ITS (for maintenance purposes only).

1.1.2 Equipment

All IT equipment within NIPEC is tagged with a unique Asset tag and logged in the NIPEC Asset location register which is linked to the NIPEC Asset Register held by BSO Finance.

For laptops, Projectors and other portable equipment, users should take note of the following security arrangements:

- Staff provided with NIPEC laptops instead of a PC in their office must secure the device to the operation cradle or desk and if this is not possible, the equipment should be placed in a secure locked location when the member of staff is out of the office.

- Users should ensure that laptops, handheld devices, mobiles, etc are kept away from magnetic sources e.g. TV, Airport Human Metal Detectors. Magnetic fields can damage hard disks and mobile phone SIM Cards - this could result in data loss/corruption.
- Caution should be exercised especially at airports, where laptops are frequently stolen. Users are reminded not to place laptops and other equipment onto

conveyor belts until the very last moment – always keeping an eye on it at all times as they walk through the metal detectors. **NEVER** carry equipment through the Airport Human Metal detector (Conveyor belt X-Ray machines are data safe).

- Laptops, Projectors and other equipment should not be left on view in an unattended car – If any staff member has a requirement to leave equipment in a car, it should always be placed in the boot.
- For the protection of NIPEC data, stored on laptops, each laptop has PGP encryption software installed, and the hard disk is encrypted. The encryption requires a password access prompt to be completed, before the laptop can be used.
- Whilst staying in a hotel, equipment (including data flash drives, although NIPEC has taken some steps to ensure that encryption is used to protect data where necessary) should never be left unattended in a hotel room. If necessary, equipment should be placed in the hotels safe.
- Staff should perform frequent backups of data stored on laptops and mobile phone directories.
- Mobile phones should be protected by the setting up of a PIN Code, which needs to be entered every time the phone is turned on.
- Protect laptop data by setting up access passwords to equipment – these should be changed regularly.

Copyright law protects all NIPEC Software. Any unauthorised copying is a violation of NIPEC Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software.

2 Purpose

This ICT Security Policy details the regional approach to ICT and Information Security Management across the HSC, including the overall management structure and key principles which apply to each HSC organisation. This will ensure a consistent and high standard of security management across the entire HSC community from all significant threats whether internal, external, deliberate or accidental.

3 Scope

This ICT Security Policy applies to:

- All parties who have access to, or use of ICT systems and information belonging to, or under the control of NIPEC, including
    - NIPEC employees
    - NIPEC Council Members
    - Temporary Staff, including agency workers
    - Business Services Organisation IT Services Unit (BSO ITS) Staff, responding to INFRA Requests, and/or who are conducting work on behalf of NIPEC
    - Third Party Contractors
    - Any other party making use of NIPEC ICT resources
- Information stored, or in use, on NIPEC ICT systems;
- Information in transit across the NIPEC Internal and/or HSC network;
- Information leaving the HSC network from NIPEC;
- ICT Systems belonging to or under the control of NIPEC.

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 ICT and Information Security Management across the HSC.

The Health and Social Care Board (HSCB) is responsible for the effective commissioning of ICT services across the HSC, 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 ICT Security management across the region through the e-Health Leads Group. This group holds responsibility for considering and proposing amendments to ICT Security management. Significant amendments will be approved by the Regional Director of eHealth 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.

4.4 Collaboration

All HSC organisations are expected to work together to ensure the successful implementation and development of ICT and information security across the HSC.

4.5 Operational Management

4.5.1 HSC ICT Security Officer Group

The HSC governs local implementation of ICT Security management across the region through an internal working group of ICT Security representatives from HSC organisations, chaired by the HSC ICT Security Manager of the Business Services Organisation.

4.5.2 Local Security Management

Each HSC organisation is responsible for implementing a local programme of ICT and 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

The Chief Executive is responsible to the DoH for the secure operation of ICT and information systems 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 and that these are appropriately assessed for security and protected.
- Ensuring the organisation maintains compliance with HSC ICT Security Policy.

4.6.2 Senior Information Risk Owner (SIRO)

Responsible to the Chief Executive (CE) 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 the following: -

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.
- Owning the organisation's information adverse incident policy.

4.6.3 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, both the Corporate Services Manager and the Corporate IT & Information Officer 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.
- Understanding and addressing risks to the asset, and providing assurance to the SIRO.

4.6.4 HSC ICT Security

Under the SLA with BSO ITS, the HCS with the assistance of the ITS Security Manager fulfils this role within NIPEC.

The BSO, ITS Security Manager is responsible for:

- Co-ordinating ICT security matters across organisational and system boundaries within the HSC.
- Monitoring the effectiveness of ICT Security Policy, procedures, standards, guidelines across the HSC.
- Taking a pro-active role in establishing and implementing an HSC-wide ICT Security Programme including training, awareness and guidance.
- Promoting ICT security awareness across the HSC.
- Receiving and considering reports of ICT Security incidents from the NIPEC SIRO and/or in his/her absence, a NIPEC IAO to ensure the necessary corrective or preventative actions are implemented.
- Liaising with the SIRO and IAOs within NIPEC on matters of ICT Security which may impact across HSC organisations.

4.6.5 HCS

Responsible to the Chief Executive, and provides a local perspective on all ICT Security matters. Within NIPEC, the HCS fulfils this role, and is responsible for the following: -

Responsible for:

- Co-ordinating ICT security matters with the assistance of ITS within the organisation.
- Monitoring the effectiveness of ICT security policy, procedures, standards, guidelines within the organisation.
- Promoting ICT security awareness across the organisation.
- Receiving and considering reports of ICT Security incidents from System Managers or others, ensuring the necessary corrective or preventative actions are implemented.
- Liaising with HSC ICT Security Manager on matters of ICT Security which may impact other HSC organisations.

4.6.6 Information Asset Adminsiatrators (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 ITS to ensure core local processes are consistently applied across all information systems.
- Ensuring users of the system are appropriately trained.
- Reporting security matters to one of the NIPEC IAOs.

4.6.7 Third Party Contractors:

Responsible to the SIRO and/or IAO by ensuring compliance to regional and local ICT Information Security Policies

Responsible for:

- Complying with the terms of their Statement of Compliance.

4.6.8 NIPEC Users

All NIPEC users are responsible for:

- Complying with all NIPEC and regional ICT and information security policies, procedures or standards.

In addition NIPEC staff are responsible for:

- Ensuring attendance at all necessary ICT and information security awareness/training sessions
- Reporting adverse incidents relating to ICT or information security to either the SIRO and/or one of the NIPEC IAOs using the NIPEC Adverse Incident Policy.

5 Policy Statement

5.1 Statement of Compliance

All HSC organisations are required to demonstrate their compliance to the current policy by submitting a Statement of Compliance signed by their Chief Executive, and

the individual with operational responsibility for monitoring and sustaining the organisations conformance to the policy.

This statement of compliance process will be overseen and managed through the HSC ICT Security Manager.

NIPEC, alongside all other HSC organisations, are required to ensure that non-HSC organisations (including 3rd party contractors) which have access to NIPEC ICT systems or information, submit statements of compliance.

- Appendix A illustrates the document to be completed by HSC Trusts, Board, BSO, Agencies and Non-Departmental Bodies.
- Appendix B illustrates an example document which could be used for non-HSC organisations.

5.2 Controls Assurance

All HSC organisations, including NIPEC, are required to achieve and maintain substantive compliance in Information and Communication Technology Controls Assurance Standard, in order to provide routine assurance that ICT and information security is being effectively managed.

5.3 Terms and Conditions of Employment

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

5.4 Authorised Use

Access to NIPEC ICT systems and information is only permitted where there is a business need.

5.5 Acceptable Use

All users of ICT systems and information (including NIPEC staff and other HSC organisations) must abide by the terms of the HSC ICT Security Policy, associated minimum security standards and applicable statements of compliance and codes of conduct.

5.6 Security Awareness

NIPEC will ensure that:

- ICT and information security awareness training is provided to all users with access to HSC ICT systems and information.
- Appropriate specialist ICT and information security training is provided to individuals working in specialised roles, as relevant to the role.
- All relevant ICT and information security policies, procedures and guidelines are developed and made available to and accessible by all users.

5.7 Risk Analysis & Management

All NIPEC users must ensure that they identify, assess and manage risks to HSC ICT systems and information and inform if required the SIRO for inclusion in the organisational Risk Register

5.8 Disaster Recovery

Under the SLA with BSO ITS, a secure backup and recovery process is in place to provide protection in the event of a system failure or incident.

5.9 Business Continuity

NIPEC has developed a Business Continuity plans (Ref: NIPEC/16/05), to maintain an adequate level of service in the event of any significant disruption to ICT or information services.

5.10 Information Sharing

All Personal data held in NIPEC information systems are safeguarded by the Data Protection Act (1998) which places obligations on those who record or use such information. NIPEC has taken account of these obligations through its Information Governance Strategy.

5.11 Outsourcing

NIPEC, in consultation with BSO ITS, will ensure that ICT & information security clauses, particularly with regards to the Data Protection Act 1998, are built into all formal service contracts.

Where data is being hosted external to the HSC network, information-based risk assessments should be considered, with regards to:

- business continuity planning
- physical & logical access management
- audit logging & access to logs/reports
- termination of contract
- disposal of information

5.12 Data Classification

All HSC organisations should establish procedures for the handling and storage of information. This is imperative in order to protect the unauthorised disclosure of such information. In general, procedures should be drawn up for handling information consistent with its classification and in line with local information governance policies.

5.13 Encryption

All sensitive data held on removable media/devices including laptops/tablets/smart phones and sent via the internet must be encrypted to the HSC approved standard as mandated by DHSSPNI.

5.14 Asset Management

All assets remain the property of NIPEC/BSO ITS.

NIPEC maintain an inventory of all digital information assets which will be managed in accordance with HSC ICT Security Policy, associated minimum security standards, and applicable statements of compliance and codes of conduct. This inventory must be managed to include updates when assets are transferred to other users or returned when a user is leaving.

5.15 Account Management

NIPEC, through their SLA with BSO ITS, ensure that procedures are in place to manage access to ICT & information systems, by way of individual user accounts. These include procedures to manage changes when staff members are transferred to other roles and removals when an employee leaves or a contract expires.

Security privileges and access rights must be allocated based on the requirements of a user's role.

5.16 Asset Maintenance

NIPEC, through their SLA with BSO ITS, will ensure that any maintenance by external third party organisations will be subject to contractual agreement, including consideration of assets that are removed from NIPEC premises for repair, with appropriate measures being taken for those devices which contain data.

As with all equipment due for repair, the sensitivity of the data and consequences of disclosure should be weighed against the need to repair rather than be disposed of or replaced.

5.17 Software Management

NIPEC, through their SLA with BSO ITS, ensure that a software maintenance routine is in place with regards to patching and the update of known vulnerabilities. This is carried out regularly (usually once a month, but sometimes more frequently) in order to minimise the associated threats.

5.18 Physical and Environmental Security

NIPEC have physical security measures for all removable equipment within the organisation, as well as an IT store which has a keypad control.

5.19 Remote Working

The Senior Team within NIPEC and Council members have access to remote working, allowing users to connect into the HSC network from home and outside NIPEC premises. This connection through BSO ITS is a multiple layer authentication through SecureClient.

5.20 Removable Media Handling

NIPEC have processes in place (detailed within NIPEC Ethical Code) to direct the use and handling of removable media, including guidance for users on physical security and the transfer of data/information.

5.21 Incident Reporting and Management

NIPEC encourages good practice incident reporting as per NIPEC's Adverse Incident Policy ref: NIPEC/16/16, covering ICT and information security incidents.

Any incidents which may impact other HSC organisations should be shared with the HSC ICT Security Manager, who will consider the impact and liaise with other HSC organisations to ensure a pro-active approach to threats.

6 Compliance (Legal / Contractual)

Legislation imposes a need for ICT security and all HSC organisations, including NIPEC, to take steps to ensure compliance with all statutory requirements. Legislation includes but is not limited to:-

- The Data Protection Act 1998
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Access to Health Records Act (1990) and Northern Ireland Order (1993)
- The Health and Safety at Work (NI) Order (1978) and Health and Safety (display Screen Equipment) Regs (NI) 1992
- The Human Rights Act (1998)
- The Employment Practices Data Protection Code
- The Obscene Publication Act 1958
- Protection of Children (NI) Order 1978
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- The Lawful Business Practice Regulations 2000

All HSC organisations, including NIPEC, must also comply with related contractual requirements, standards and principles in the following areas:

- Intellectual Property Rights (IPR)
- Protection of Organisational Records
- Protection & privacy of personal information
- Prevention of misuse of Information Processing Facilities
- Management and regulation of cryptographic controls

7 Monitoring

NIPEC reserve the right to monitor the use of HSC ICT systems, devices and information in order to ensure compliance with relevant policies and to protect the confidentiality, integrity and availability of information assets.

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.

All HSC organisations should, at their discretion, or where required by law, report relevant ICT or information security incidents/threats to the appropriate UK authorities for further investigation where necessary.

8 Non-Compliance / Policy Breaches

An information security breach is defined by ISO/IEC 27035:2011 as “*an identified occurrence of a system service or network state indicating a possible breach of information security policy or failure of safeguards*”

An incident is an event that has a high probability of compromising the business operations or other information security impact. A weakness is the potential for an

incident to occur that was previously unknown or not considered during a risk analysis.

Both incidents and weaknesses are considered breaches and have potential to affect confidentiality, integrity and availability of HSC information; result in financial penalties or negatively impact the reputation of the HSC therefore:

8.1 Sanctions:

8.1.1 Failure of HSC Organisations

Where an HSC organisation is found to be in breach of HSC policy, it is expected that that HSC organisation will investigate in accordance with Adverse Incident procedures and report their findings to the internal ICT management framework group.

If the breach is deemed significant enough to put the 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.

Where serious breaches have occurred it may also be necessary to report to the Information Commissioners Office or other appropriate regulatory bodies.

8.1.2 Failure of NIPEC Employees

Where a NIPEC employee is found to be in breach of this policy, NIPEC will investigate in accordance with 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.

8.1.3 Failure of third parties, temporary/agency staff etc

Where a third party, temporary/agency person is found to be in breach of this policy, NIPEC will investigate in accordance with 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 Security Policy Review

NIPEC will adhere to HSC ICT Security Policy, which is published by the HSCB and will be maintained through the HSC ICT Security Manager.

It is accepted that the HSC ICT Security Policy will be subject to an annual review or following any significant incidents, changes to UK or EU legislation or changes to the HSC structure or functional responsibilities. Any changes to the HSC policy, will therefore require to be reflected within this policy, so therefore this NIPEC Policy is also subject to regular review and will take into account any changes to the HSC ICT Security Policy.

10 References

- Cabinet Office - Security policy framework (April 2014)
- Cabinet Office – Government Security Classifications (April 2014)
- DHSSPS - Code of Practice on Protecting the Confidentiality of Service User Information (January 2012)
- DHSSPS – Information and Communication Technology Controls Assurance Standards (2008/9)
- DHSSPS & HSC Protocol For Sharing Service User Information for Secondary Purposes (August 2011)
- Health and Social Care Information Centre - Information Governance Statement of Compliance process
- Information Commissioners Office - Employment Practices Code Part 3: Monitoring at Work
- International Organization for Standardization - ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.
- Protection of Children (Northern Ireland) Order 1978

Appendix A

Statement of Compliance to the HSC Network

for

HSC Trusts, Board, BSO, Agencies

and Non-Departmental Bodies

Statement of Compliance to the HSC Network

This Statement of Compliance is a minimum requirement and for particular organisations or applications and may be supplemented by additional requirements identified by the Health Social Care Board.

I .....of .....

(name of CEO or equivalent) (HSC Organisation name)

certify that the following security measures are in place and will be adhered to:

The following represents the baseline requirements for connection to the HSC network and conformance to published policy on matters relating to the security of information held within, or communicated across the HSC ICT infrastructure.	
1. The organisation abides by the HSC ICT Security Policy and associated documentation. 2. The organisation understands the need to assess risk and to implement measures to ensure the preservation of confidentiality, integrity and availability of information. 3. Senior Management within the organisation have set clear policy direction through the issue and maintenance of an Information Security policy. 4. The organisation has established a management framework to initiate and control the implementation of information security within the organisation. 5. The organisation has established processes to ensure that the organisation's assets are effectively protected. 6. The organisation has defined ICT security roles and responsibilities throughout the organisation and has established mechanisms to ensure that all staff within the organisation's employ are properly informed of the role they play in maintaining the ICT security of the organisation.	7. The organisation has implemented measures to prevent unauthorised access, damage and interference to organisation premises, equipment and information. 8. The organisation has implemented Communications and Operations Management measures to ensure the correct and secure operation of information processing facilities. 9. The organisation has implemented measures to control access to information for both staff within the organisation's employ and other external individuals and third party organisations that may be granted access to the organisation's ICT infrastructure. 10. The organisation has implemented measures to ensure that security is built into information systems. 11. The organisation has implemented measures to counteract interruptions to business activities and to protect critical business processes from the effects of major failure or disasters. 12. The organisation's design, operation, use and management of information systems comply with current relevant criminal and civil law and statutory, regulatory and contractual obligations.

Signature

I certify that the above is true and understand that continuing failure to meet some or all parts of this Statement of Compliance may result in disconnection from the HSC network.

Signature..... **Date**.....

The signatory must carry the specific authority of the Chief Executive or equivalent

Name.....

Postion.....

Signature..... **Date**.....

This must be countersigned bythe nominated individual responsible for ICT Security

Name.....

Postion.....

Any significant changes in the status of the organisation should be communicated to the HSC ICT Security Manager (ictsecuritymanager@hscni.net).

Appendix B

Statement of Compliance to the HSC Network

for

Third Parties

Third Party N3 Remote Access Service Statement of Compliance

This statement of compliance is a minimum requirement for third party contractors to be granted access to the HSC N3 Remote Access Service. This may be supplemented by additional requirements identified by the HSC Business Services Organisation.

Conditions of Access

Remote access is granted under the following conditions:-

- Access shall be used only to provide the services previously agreed with the HSC organisation to which access has been authorised.

- An individual access session shall only be used to access HSC systems directly – i.e. it is not permitted to use a direct session to any HSC system to access any other host or network from that system. Where an exception to this condition is required it must be first agreed with the HSC ICT Security Manager.

- Any incidents or circumstances of which you/your organisation become aware that may endanger the security of the HSC Network shall be immediately reported to the HSC ICT Security Manager.

I hereby confirm that ***<insert organisation name here>*** have read, agree and comply with the terms and conditions stated in this Statement of Compliance and acknowledge that failure to maintain compliance with the Statement of Compliance may result in the withdrawal of access to the HSC network.

Signature..... **Date**.....

The signatory must carry the specific authority of the Managing Director or equivalent

Name.....

Postion.....

When completed an electronic version should be emailed to the HSC ICT Security Manager at ictsecuritymanager@hscni.net.

Third Party SSL Remote Access Service Statement of Compliance

This statement of compliance is a minimum requirement for third party contractors to be granted access to the HSC SSL Remote Access Service. This may be supplemented by additional requirements identified by the HSC Business Services Organisation (BSO).

Conditions of Access

Remote access is granted under the following conditions:-

- Access shall be used only to provide the services previously agreed with the HSC organisation to which access has been authorised

- An individual access session shall only be used to access HSC systems directly – i.e. it is not permitted to use a direct session to any HSC system to access any other host or network from that system. Where an exception to this condition is required it must be first agreed with the HSC ICT Security Manager.

- Access to any part of the HSC network is not permitted other than by using strong authentication.

- Any incidents or circumstances of which you/your organisation become aware, including loss of the authentication token supplied by the BSO, that may endanger the security of the HSC Network shall be immediately reported to the HSC ICT Security Manager.

- Your organisation will provide one or more static public IP address/es and not use NAT traversal

- Your organisation must connect from a PC that meets the standards defined by in the Third Party SSL Remote Access - Minimum Device Standards document issued by BSO.

- The authentication tokens remain the property of the BSO and must be returned if so requested by the HSC ICT Security Manager

I hereby confirm that ***<insert organisation name here>*** have read, agree and comply with the terms and conditions stated in this Statement of Compliance and acknowledge that failure to maintain compliance with the Statement of Compliance may result in the withdrawal of access to the HSC network.

Signature..... **Date**.....

The signatory must carry the specific authority of the Managing Director or equivalent

Name.....

Postion.....

When completed an electronic version should be emailed to the HSC ICT Security Manager at ictsecuritymanager@hscni.net.

Third Party Gateway VPN Remote Access Service Statement of Compliance

This statement of compliance is a minimum requirement for Third Party Contractors to be granted access to the HSC Gateway VPN Remote Access Service. This may be supplemented by additional requirements identified by the HSC Business Services Organisation (BSO).

Conditions of Access

Remote access is granted under the following conditions:-

- Access shall be used only to provide the services previously agreed with the HSC organisation to which access has been authorised.

- An individual access session shall only be used to access HSC systems directly – i.e. it is not permitted to use a direct session to any HSC system to access any other host or network from that system. Where an exception to this condition is required it must be first agreed with the HSC ICT Security Manager.

- Access to the HSC wide area network and to any HSC organisation local area network is not permitted other than by using strong authentication.

- Any incidents or circumstances of which you/your organisation become aware, including loss of the authentication token supplied by the BSO, that may endanger the security of the HSC Network shall be immediately reported to the HSC ICT Security Manager.

- Your organisation has a Common Criteria EAL4 certified firewall as the VPN end point on the connection to the HSC network.

- Your organisation will provide one or more static public IP address/es and not use NAT traversal.

- The authentication tokens remain the property of the BSO and must be returned if so requested by the HSC ICT Security Manager.

I hereby confirm that ***<insert organisation name here>*** have read, agree and comply with the terms and conditions stated in this Statement of Compliance and acknowledge that failure to maintain compliance with the Statement of Compliance may result in the withdrawal of access to the HSC network.

Signature..... **Date**.....

The signatory must carry the specific authority of the Managing Director or equivalent

Name.....

Postion.....

When completed an electronic version should be emailed to the HSC ICT Security Manager at ictsecuritymanager@hscni.net.

Third Party Bomgar Remote Access Service Statement of Compliance

This statement of compliance is a minimum requirement for Third Party Contractors to be granted access to the HSC Gateway VPN Remote Access Service. This may be supplemented by additional requirements identified by the HSC Business Services Organisation (BSO).

Conditions of Access

Remote access is granted under the following conditions:-

- Access shall be used only to provide the services previously agreed with the HSC organisation to which access has been authorised.

- An individual access session shall only be used to access HSC systems directly – i.e. it is not permitted to use a direct session to any HSC system to access any other host or network from that system. Where an exception to this condition is required it must be first agreed with the HSC ICT Security Manager.

- Access to the HSC wide area network and to any HSC organisation local area network is not permitted other than by using strong authentication.

- Any incidents or circumstances of which you/your organisation become aware, including loss of the authentication token supplied by the BSO, that may endanger the security of the HSC Network shall be immediately reported to the HSC ICT Security Manager.

- The HSC Bomgar management console software and authentication tokens remain the property of the BSO and must be returned if so requested by the HSC ICT Security Manager.

- The HSC Bomgar management console must only be used to support HSC organisations.

I hereby confirm that ***<insert organisation name here>*** have read, agree and comply with the terms and conditions stated in this Statement of Compliance and acknowledge that failure to maintain compliance with the Statement of Compliance may result in the withdrawal of access to the HSC network.

Signature..... **Date**.....

The signatory must carry the specific authority of the Managing Director or equivalent

Name.....

Postion.....

When completed an electronic version should be emailed to the HSC ICT Security Manager at ictsecuritymanager@hscni.net.