Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.08 Encryption All User Standard

Approval

Document Reference	Information Security - 1.08 Encryption - All User Standard
Version	0.3
Last updated	1st March 2021
Owner	
Approval by	

Contents

1. INTRODUCTION

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

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

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

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

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

2. PURPOSE

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

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

3. SCOPE

This Information Security Standard applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS [1], including:

[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

    - HSC and NIFRS employees;
    - Temporary Staff including agency and students;
    - Voluntary Health Sector organisations / Volunteers;
    - Third Party Contractors;
    - Any other party making use of HSC ICT resources;
- HSC information stored, or in use, on HSC or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving HSC networks; and
- ICT Systems belonging to or under the control of HSC.

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

4. STANDARD NON-COMPLIANCE / BREACH

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

5. ENCRYPTION

5.1. Management of Encryption at HSC

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

- Information classified as personally identifiable or business sensitive is being processed or shared using a digital device(s), including:
    - HSC computer systems, and mobile and tablet devices
    - Protection of secret authentication information (e.g. passwords, cryptographic keys and pins);
    - Electronic transaction data (e.g. payment information, credit cards etc);
    - Where local laws or regulations mandate;
- Digital devices and/or storage media has the potential to store personally identifiable information;
- Digital data is being shared over an untrusted network (a network that HSC has no control or assertions as to it level of security i.e. the internet);
- Digital data is being transferred using storage media (such as physical hard drive, backup media, USB memory sticks, SD cards, optical media etc.); and

(NIPEC), NI Medical and Dental Training Agency (NIMDTA), GP Practices and other Independent Contractors to HSC, and Northern Ireland Fire and Rescue Service.

- As otherwise identified as necessary by a risk assessment.

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

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

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

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

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

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

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

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

5.2. Technical Encryption Requirements

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

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

encryption.

5.2.3. Bring Your Own Devices (BYOD) are not permitted.

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

5.2.5. Any storage devices connecting to the system will be blocked [IS1]unless encryption is in place, such as with BitLocker full disk encryption with AES encryption algorithm and a 256-bit key[IS2].

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

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

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

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

5.3. Email Specific Requirements

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

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

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

5.3.3. HSC has agreed processes that cover all types of domains that must be followed when sharing information via email. See appendix 1 for detailed instruction as to the treatment of email being sent to specific domains and the type of encryption

required. Appendix 1 includes instructions for the following :

- Northern Ireland Government Departments - *nigov.net, *ni.gov.uk, @ccea.org.uk, @hiainquiry.org and @sportscouncil-ni.org.uk @ihrdni.org, @nipso.org.uk;
- NI Civil Service network;
- UK Mainland Government Departments - , *.gov.uk, *.gsi.gov.uk;
- Private government network;
- Inbound via the internet;
- Police - *.pnn.police.uk;
- UK NHS - *.nhs.uk and @nhs.net;
- Criminal Justice Secure Mail - *.cjsm.net;
- HSC email - *.hscni.net and n-i.nhs.uk;
- All other email domains.

5.3.4. Domains in the table below must ensure an encrypted connection is established between the HSC exchange and the below domain's exchange (for example using at least TLS v1.2) when sending email via the internet:

Mail domain	**Description**
@antrimandnewtownabbey.gov.uk%%	Antrim and Newtownabbey Council
@armaghbanbridgecraigavon.gov.uk%%	Armagh Banbridge and Craigavon Council
@askmygp.com%%	Ask My GP
@beaumont.ie%%	Beaumont Hospital
@belfastcity.gov.uk%%	Belfast City Council
@boi.com%%	Bank of Ireland
@boots.co.uk%%	Walgreens Boots Alliance
@cathedraleye.com%%	Cathedral Eye Clinic
@causewaycoastandglens.gov.uk%%	Causeway Coast and Glens Council
@healthmail.ie%%	Health Mail Service for Ireland
@hrconnect.nigov.net	Northern Ireland Civil Service Recruitment
@kingsbridgehealthcaregroup.com%%	Kingsbridge Private Hospital
@lisburncastlereagh.gov.uk%%	Lisburn and Castlereagh Council
@midandeastantrim.gov.uk%%	Mid and East Antrim Council
@midulstercouncil.org%%	Mid Ulster Council
@niwh.co.uk%%	North West Independent Clinic
@nmand.org%%	Newry Mourne and Down Council
@uic.org.uk%%	Ulster Independent Clinic
@wiggly-amps.com%%	Wiggly Amps

5.4. Managing Electronic Keys

5.4.1. Each local HSC IT Department is responsible for the management of encryption

keys throughout the key lifecycle.

5.4.2. A key management system should be used based on the local organisation's requirements for:

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

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

5.4.4. Only encryption tools approved by your local ICT department may be used on Trust devices. These tools may vary between Trusts.

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

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

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

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

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

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

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

5.4.12. PKI infrastructure must use an offline, and stand-alone, root certificate authority

(CA), which adheres to NCSC guidance.

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

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

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

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

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

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

5.4.19. Keys must never be stored on the same system as the information they are used to encrypt/decrypt.

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

5.4.21. Archived keys must be stored separately from active keys.

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

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

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

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

6. MONITORING

6.1.1. 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.

6.1.2. 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.

7. REVIEW CYCLE

This standard 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.

<<Add Name>>.

<<Add Role>> Date: 02/03/2020

<<Add Name>>.

<<Add Role>> Date: 02/03/2020

8. APPENDIX 1

Detailed instruction as to the treatment of email being sent to specific domains.

Email Domains	Email without Password Protection	Password Protect Email and associated documentation	Encrypt email and associated documentation
Northern Ireland Government Departments - *nigov.net, *ni.gov.uk, @ccea.org.uk, @hiainquiry.org and @sportscouncil-ni.org.uk @ihrdni.org, @nipso.org.uk			
Outbound is via the HSC private connection to the NI Civil Service network.	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Inbound is via the HSC private connection to the NI Civil Service network.	If the email does not contain Person identifiable/Trust sensitive Information	Advise sender to Password protect if the email contains Person identifiable/Trust sensitive information.	Advise sender to Password protect if the email contains Person identifiable/Trust sensitive information.
UK Mainland Government Departments - , *.gov.uk, *.gsi.gov.uk			
Outbound is via the HSC private connection to the NI Civil Service network and onward via the private government network.	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Inbound is via the internet.	If the email does not contain Person identifiable/Trust sensitive Information	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.
Police - *.pnn.police.uk			

Email Domains	Email without Password Protection	Password Protect Email and associated documentation	Encrypt email and associated documentation
Outbound is via the internet.	Encrypt if the email contains Person identifiable/Trust sensitive information.	Encrypt if the email contains Person identifiable/Trust sensitive information.	Encrypt if the email contains Person identifiable/Trust sensitive information.
Inbound is via the internet.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.
UK NHS - *.nhs.uk and @nhs.net			
Outbound is via the internet.[DJ3]	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Inbound to hscni.net mailboxes is via the internet.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.
Inbound to n-i.nhs.uk is via the HSC private connection to the N3 network	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Criminal Justice Secure Mail - *.cjsm.net			

Email Domains	Email without Password Protection	Password Protect Email and associated documentation	Encrypt email and associated documentation
Outbound is via an encrypted VPN over the internet to CJSM network.	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Inbound is via an encrypted VPN over the internet from the CJSM network	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
HSC email - *.hscni.net and n-i.nhs.uk			
Outbound never leaves the HSC private network	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
Inbound never leaves the HSC private network	If the email does not contain Person identifiable/Trust sensitive Information	Password protect if the email contains Person identifiable/Trust sensitive information.	Password protect if the email contains Person identifiable/Trust sensitive information.
All other email domains			
Outbound is via the internet.	If the email does not contain Person identifiable/Trust sensitive Information	Encrypt if the email contains Person identifiable/Trust sensitive information.	Encrypt if the email contains Person identifiable/Trust sensitive information.
Inbound is via the internet	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.	Advise sender to encrypt if the email contains Person identifiable/Trust sensitive information.