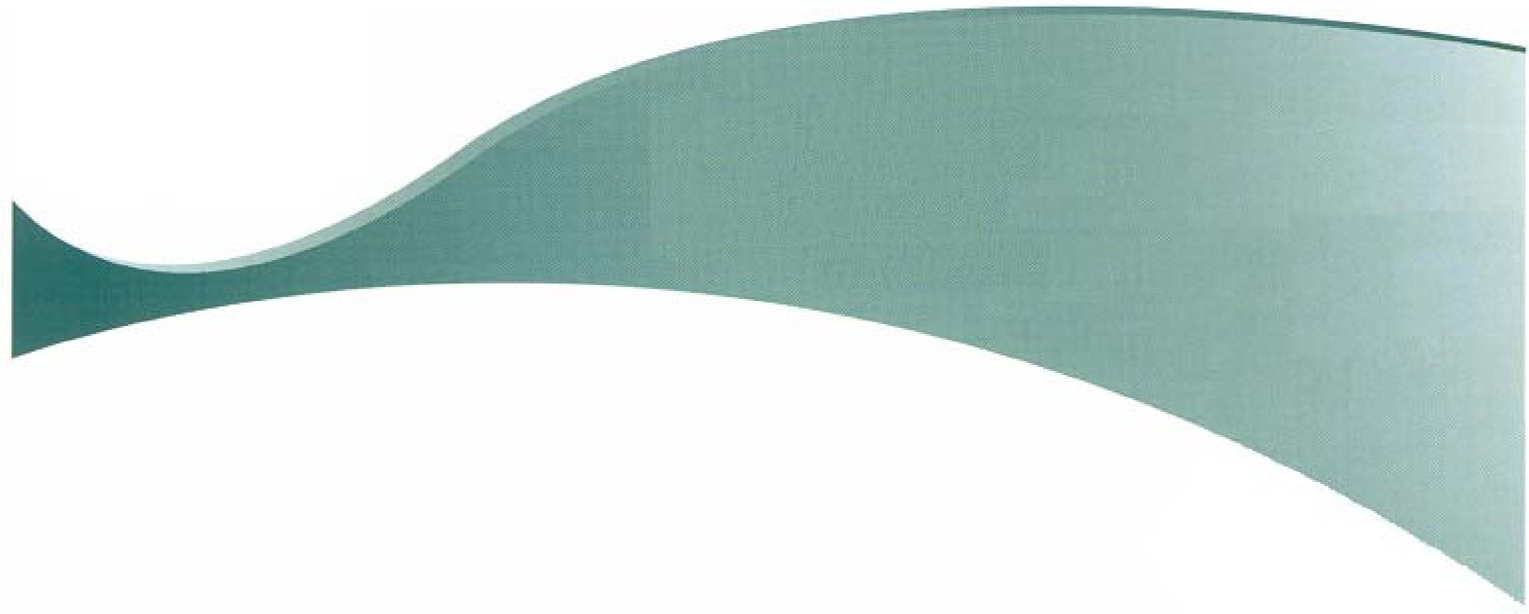
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Encryption Policy



Version 3.0

This policy maybe updated at anytime (without notice) to ensure changes to the HSE's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check the HSE intranet for the most up to date version of this policy

http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

Reader Information

Title:	HSE Encryption Policy.
Purpose:	To define the acceptable of use and management of encryption throughout the HSE.
Author:	Information Security Project Board (ISPB) on behalf of the HSE.
Publication date:	February 2013
Target Audience:	All users (including HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the HSE's I.T resources.
Superseded Documents:	All local encryption policies and procedures.
Related Documents:	HSE Information Security Policy. HSE Information Technology Acceptable Use Policy. HSE Electronic Communications Policy. HSE Password Standards Policy.
Review Date:	February 2014
Contact Details:	Chris Meehan ISPB Secretary, ICT Directorate Dr.Steevens Hospital Steevens Lane Dublin 8 Email: chris.meehan@hse.ie

Document History

Version	Owner	Author	Publish Date
1.0	HSE	Information Security Project Board (ISPB)	June 2009
2.0	HSE	Information Security Project Board (ISPB)	November 2010
2.5	HSE	Information Security Project Board (ISPB)	July 2012
3.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout the Health Service Executive (HSE).

This policy is mandatory and by accessing any Information Technology (I.T.) resources which are owned or leased by the HSE, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the HSE's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All Information Technology (I.T.) resources provided by the HSE;
- All users (including HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the HSE's I.T resources;
- All connections to (locally or remotely) the HSE network Domains (LAN/WAN/WiFi);
- All connections made to external networks through the HSE network..

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A.*

4.0 Policy

4.1 Principles of Encryption

- Where possible all confidential and restricted information must be stored on a secure HSE network server with restricted access. Where it has been deemed necessary by a HSE line manger (at grade 8 level (or equivalent) or above) to store confidential or restricted information on any device other than a HSE network server the information must be encrypted.
- All confidential and restricted information transmitted via email to an email address outside of the HSE domain (i.e. one that does **<u>not</u>** end in "@hse.ie") must be encrypted.

- All passwords used as part of the process to encrypt/decrypt information must meet the requirements of the ***HSE Password Standards Policy*** (*http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf*).

4.2 Servers

- Confidential and restricted information stored on shared HSE network servers which are situated in physically insecure locations (For example remote file/print servers) must be protected by the use of strict access controls and encryption software.

4.3 Desktop Computers

- HSE desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However the following types of HSE desktop computers will need to have encryption software installed:

  1) Desktop computers which for business, geographic or technical reasons need to permanently store HSE confidential or restricted information locally on the computers hard drive (as opposed to a secure HSE network server).

  2) Desktop computers which for business, geographic or technical reasons need to permanently host HSE information systems (for example, MS Access, Excel etc) that process HSE confidential or restricted information locally on the computers hard drive (as opposed to a secure HSE network server).

  3) Desktop computers used by HSE staff to work from home (home working).

  4) Desktop computers which are located in unrestricted areas which are open to the public (for example: reception desks etc).

  5) Desktop computers which are located in third party facilities.

- The preferred method of encryption for HSE desktop computer devices is whole disk encryption.

4.4 Laptop, Mobile Computer & Smart Devices

- All HSE laptop computer devices must have HSE approved encryption software installed prior to their use within the HSE. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.

- HSE mobile computer devices & smart devices must have device encryption enabled or HSE approved encryption software installed prior to their use within the HSE.

- The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

- Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

4.5 Removable Storage Devices

- All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

- Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

- The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

4.6 USB Memory Sticks

- Confidential and restricted information may only be stored on **HSE approved encrypted USB memory sticks** which are available from the ICT Directorate. The storage of confidential or restricted information on any other USB memory sticks (encrypted or otherwise) will be considered a breach of this policy.

- HSE approved USB memory sticks must only be used on an **exceptional** basis where it is essential to store or temporarily transfer confidential or restricted information. They must **not be used for the long term storage of confidential or restricted information,** which must where possible be stored on a secure HSE network server.

- Confidential and restricted information stored on the HSE approved USB memory stick must not be **transferred** to any internal (except a secure HSE network server) or external system in an **unencrypted form**.

4.7 Transmission Security

- All confidential or restricted information transmitted through email to an email address outside of the HSE domain (i.e. one that does **not** end in "@hse.ie") must be encrypted. The transfer of such information outside of the HSE domain must abe authorised by a HSE line manager (at grade 8 level or above). The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

- Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channels (for example: Secure FTP, TLS, VPN etc). The transfer must be authorised by a HSE line manager (at grade 8 level or above). The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

- All confidential and restricted information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy) or better. All new wireless networks installations must be encrypted using WPA (Wi-Fi Protected Access) or better.

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

- The selection and procurement of all encryption facilities used within the HSE.

- The provision, deployment and management of encryption facilities within the HSE.
- The provision of training, advice and guidance on the use of encryption facilities within the HSE;

5.2 Information Owners

Information owners are responsible for:

- The implementation of this policy and all other relevant policies within the HSE directorate or service they manage;

- The ownership, management, control and security of the information processed by their directorate or service on behalf of the HSE;

- The ownership, management, control and security of HSE information systems used by their directorate or service to process information on behalf of the HSE;

- Maintaining a list of HSE information systems and applications which are managed and controlled by their directorate or service.

- Making sure adequate procedures are implemented within their directorate or service, so as to ensure all HSE employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

- Making sure adequate procedures are implemented within their directorate or service to ensure compliance of this policy and all other relevant policies;

5.3 Users

Each user of the HSE’s IT resources is responsible for:

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation.

- Respecting and protecting the privacy and confidentiality of the information they process at all times.

- Complying with instructions issued by the ICT Directorate on behalf of the HSE.

- Ensuring all encryption passwords assigned to them are kept confidential at all times and not shared with others;

- Ensuring encryption passwords used to access encrypted devices are not written down on the encrypted device or stored with or near the encrypted device;

- Reporting all misuse and breaches of this policy to their line manager.

5.4 Line Managers

In addition to each user’s responsibilities, line managers are directly responsible for:

- The implementation of this policy and all other related HSE policies within the business areas for which they are responsible.

- Ensuring that all HSE employees who report to them are made aware of and are instructed to comply with this policy and all other relevant HSE policies.

- Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

6.0 Approved Encryption Algorithms and Protocols

6.1 Symmetric Key Encryption Algorithms

- Triple Data Encryption Standard (3DES)
  (Minimum encryption key length of 168 bits)

- Advanced Encryption Standard (AES)
  (Minimum encryption key length of 256 bits)

- Blowfish
  (Minimum encryption key length of 256 bits)

6.2 Asymmetric Key Encryption Algorithms

- Digital Signature Standard (DSS)
- Rivest, Shamir & Adelman (RSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

6.3 Encryption Protocols

- IPSec (IP Security)
- SSL (Secure Socket Layer)
- SSH (Secure Shell)
- TLS (Transport Layer Security)
- S/MIME (Secure Multipurpose Internet Extension)

6.4 Encryption Key Management

- Key management must be fully automated
- Private keys must be kept confidential
- Keys in transit and storage must be encrypted

7.0 Enforcement

- The HSE reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. HSE staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.

- Breaches of this policy by a third party commercial service providers, may lead to the withdrawal of HSE information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the HSE and the third party commercial service provider.

- The HSE will refer any use of its I.T. resources for illegal activities to the Gardai.

8.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to the HSE's organisation structure and business practices are properly reflected in the policy.

The most up to date version of this policy is published on the intranet (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/).

Appendix A

Asymmetric Key Encryption Algorithms: A class of encryption algorithm in which two different keys are used: one for encrypting the information, and one for decrypting the information (Public-key encryption).

Authorisation / Authorised: Official HSE approval and permission to perform a particular task.

Confidential information: (As defined by the *HSE information Classification & Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, HSE policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the HSE, its patients, its staff and its business partners. Some examples of confidential information include:

- Patient / client / staff personal data (Except that which is restricted)
- Patient /client / staff medical records (Except that which is restricted)
- Unpublished medical research
- Staff personal records
- Financial data / budgetary Reports
- Service plans / service performance monitoring reports
- Draft reports
- Audit reports
- Purchasing information
- Vendor contracts / Commercially sensitive data
- Data covered by Non-Disclosure Agreements
- Passwords / cryptographic private keys
- Data collected as part of criminal/HR investigations
- Incident Reports

Decryption / Decrypt: The process of decoding information which has been converted into an unreadable form (cipher text) back into a readable form (plain text).

HSE Network: The data communication system that interconnects different HSE Local Area Networks (LAN) and Wide Area Networks (WAN)

HSE Network Server: A computer on the HSE network used to manage network resources.

Home Worker(s): HSE employee(s) who is authorised to work from their home (on an occasional or regular basis) instead of a HSE facility.

Home Working: The situation where HSE employees carry out their contractual obligations (either on an occasional or regular basis) on behalf of the HSE while working from their home instead of a HSE facility.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a HSE directorate or service (HSE RDO, National Director **(**or equivalent)).

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the HSE.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone.

Personal information: Information relating to a living individual (HSE employee, client and patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information;
- Collecting, organising, storing, altering or adapting the information;
- Retrieving, consulting or using the information;
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the information.

Removable storage Device: Any optical or magnetic storage device or media including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external hard drives.

Restricted Information: (As defined by the *HSE information Classification & Handling Policy*) Highly sensitive confidential information**.** The unauthorised or accidental disclosure of this information would seriously and adversely impact the HSE, its patients, its staff and its business partners. Some examples of restricted information include:

- Patient / client / staff sensitive personal information (i.e. mental health status, HIV status, STD/STI status etc)
- Childcare / Adoption information
- Social Work information
- Addiction Services information
- Disability Services information
- Unpublished financial reports
- Strategic corporate plans
- Sensitive medical research

Smart Device: A handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing etc. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc).

Symmetric Key Encryption Algorithms: A class of encryption algorithm in which the same key is used for both encryption and decryption of the information.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the HSE to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the HSE.

Transmission / Transmitted: The process of sending something (information or otherwise) from one location to another location.

Whole Disk Encryption: A method encryption where the entire contents (bits & bytes) of a magnetic or optical disk are encrypted.