Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Information Technology (I.T.) Security 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/

Document Information

Title:	HSE Information Technology (I.T.) Security Policy.
Purpose:	This is a general statement of policy in respect of Information Technology (I.T.) security for the HSE.
Author:	Information Security Project Board (ISPB) on behalf of the HSE.
Publication date:	February 2013
Target Audience:	All HSE staff, students, contractors, sub-contractors, agency staff and authorized third parties that use the organizations IT resources.
Superseded Documents:	All relevant local HSE information security policies.
Related Documents:	*HSE Information Technology Acceptable Use Policy*. *HSE Electronic Communications Policy.* *HSE Password Standards Policy.* *HSE Encryption Policy.* *HSE Access Control Policy.* *HSE Remote Access Policy.* *HSE Mobile Phone Device Policy.* *HSE Data Classification & Handling Policy.* *HSE Data Protection Breach Management Policy.* *HSE Internet Content Filter Standard.* *HSE Service Provider Confidentiality Agreement.* *HSE Third Party Network Access Agreement.*
Review Date:	February 2014
Contact Details:	Chris Meehan ISPB Secretary, 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
3.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

The use of computer systems and the exchange of information electronically have increased rapidly in the area of healthcare. Within the HSE there is a growing reliance on computer systems to aid treatment, expand communications, and improve management and control. This growing dependence comes at a time when the number of threats and actual attacks on these computer systems is constantly increasing.

Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected information is essential to the successful operation of the HSE in the provision of services to our customers.

The purpose of this Information Technology (I.T.) Security Policy and its supporting policies, standards and guidelines is to define the security controls necessary to safeguard HSE information systems and ensure the security, confidentiality, availability and integrity of the information held therein.

This policy is mandatory and by accessing any information or Information Technology (IT) 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 is authorised by HSE Senior Management Team and represents the HSE's national position. The policy takes precedence over all other relevant policies which may have been developed at a local level.

This policy applies to all HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers that use the organizations I.T. resources and/or process information on behalf of the HSE.

3.0 Legislation

The HSE has an obligation to abide by all relevant Irish legislation and European legislation. The relevant acts, which apply in Irish law to Information Systems, include but are not limited to:

- *The Data Protection Acts (1988/2003)*
- *European Communities Data Protection Regulations, (2001)*
- *European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)*
- *Data Protection EU Directive 95/46/EC*
- *Freedom of Information Acts (199/2003)*
- *Criminal Damages Act (1991)*

- *Child Trafficking and Pornography Act (1998)*
- *Intellectual Property Miscellaneous Provisions Act (1998)*
- *Copyright and Related Rights Act (2000)*
- *Criminal Justice (Theft & Fraud Offences) Act 2001*
- *Electronic Commerce Act (2000)*
- *ECommerce Directive (2000/31/EC)*

4.0 Definitions

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

5.0 Policy

It is the policy of the HSE to: -

- Implement human, organisational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems and the information held therein;

- Develop and maintain appropriate policies, procedures and guidelines to effect a high standard of information technology security, reflecting industry best practice;

- Monitor, record and log all activity on the HSE network and use of its information technology resources

- Comprehensively assess and manage risks to HSE information systems and the information held therein;

- Continuously review and improve HSE information technology security controls, and rapidly determine the cause of any breach of security and minimize damage to information systems should any such incident occur;

- Comply with all laws and regulations governing information technology security;

- Establish information technology security education and awareness initiatives within the HSE.

6.0 Supporting Policies, Standards and Guidelines

There are a number of supporting HSE policies, standards and guidelines to accompany this policy document. Each of these accompanying policies, standards and guidelines is published on the HSE intranet and covers a specific area of information security.

All HSE staff, students, contractors, sub-contractors, agency staff and third party commercial service providers authorised to use the HSE's Information Technology (I.T.) resources are required to familiarise themselves with these accompanying policies, standards and guidelines and to work in accordance with them.

The following is a list of the accompanying policies, standards and guidelines.

6.1 Information Technology (I.T.) Acceptable Use Policy

The *Information Technology Acceptable Use Policy* outlines the correct and proper manor in which the HSE's Information Technology (I.T.) resources are to be used. It covers the following areas:

- The use of computer accounts and passwords;
- Confidentiality and privacy of information;
- The use of computer hardware and software;
- The use of laptop computers and other mobile computer devices;
- The security of HSE information, systems and computer devices;
- Lost, stolen and damaged computer devices;
- The use of the HSE telephone system;
- Storage of information;
- Backup of information;
- Security of information;
- Transfer and transport of information;
- Disposal of information;
- Tele-working / home-working;
- Virus & Malicious Software Protection
- The unacceptable use of HSE information technology resources

6.2 Electronic Communications Policy

The *Electronic Communications Policy* outlines the correct and proper manor in which the HSE's Email, Internet and facsimile (fax) facilities are to be used. It covers the following areas:

- The confidentiality and privacy of email and fax messages;
- The use of the HSE email, internet and facsimile (fax) facilities;
- The transmission of confidential or personal information via email, internet and fax;
- The legal status of HSE email and fax messages;
- The use and ownership of HSE email accounts;
- The use of third party and web based email facilities;
- Access to restricted and blocked internet content;
- The installation or use of third party internet facilities;

- The unacceptable use of HSE email, internet and facsimile (fax) facilities.

6.3 Password Standards Policy

The *Password Standards Policy* outlines the standard for the creation and use of secure passwords for use on the HSE's Information Technology (IT) resources. It covers the following areas:

- The creation of secure passwords;
- Minimum password length;
- Composition and complexity of passwords;
- The use and security of passwords.

6.4 Encryption Policy

The *Encryption Policy* outlines the acceptable use and management of encryption software throughout the Health Service Executive (HSE). It covers the following areas:

- Minimum level of encryption;
- Approved Encryption Algorithms and Protocols;
- Encryption of HSE computer devices;
- Encryption of HSE storage devices;
- Encryption of HSE email and internet messages and traffic;
- Encryption of HSE wireless network traffic.

6.5 Access Control Policy

The *Access Control Policy* outlines the correct use and management of user level access controls within the HSE. It covers the following areas:

- Ownership and management of HSE information systems and networks;
- Access to HSE information systems and networks;
- Access Account privileges;
- Access Account registration;
- Access Account management;
- Access Account de-registration;
- Access Security;
- Monitoring and review of access account privileges.

6.6 Remote Access Policy

The *Remote Access Policy* outlines the standard for connecting to the HSE network from a computer or device located outside of the HSE network. It covers the following areas:

- Remote access registration and management;
- Third party remote access registration and management;
- Security of remote access devices;
- Monitoring and security of remote access connections.

6.7 Mobile Phone Device Policy

The *Mobile Phone Device Policy* outlines the acceptable use and management of HSE mobile phone devices. It covers the following areas:

- Criteria for assignment of HSE mobile phone devices;
- Approval of assignment, upgrade and replacement of mobile phone devices;
- Procurement of mobile phones devices;
- Usage requirements and restrictions
- Security;
- Confidentiality & Privacy;
- Lost or stolen mobile phone devices;
- Disposal of mobile phone devices;
- Monitoring of mobile phone device usage;
- Processing of mobile phone device bills
- Health and safety;

6.8 Information Classification & Handling Policy

The *Data Classification & Handling Policy* outlines how HSE information must be classified and handled according to its sensitivity. It covers the following areas:

- The different classifications of HSE Information;
- How each class of information should be handled and processed;

6.9 Data Protection Breach Management Policy

The *Data Protection Breach Management Policy* outlines the approved management approach to be followed in the event of a HSE data protection breach. It covers the following areas:

- Identification and classification of a breach;
- Containment and recovery;
- Risk assessment;
- Notification of a breach;
- Evaluation and response.

6.10 Internet Content Filter Standard

The *Internet Content Filter Standard* outlines the categories of internet content which are accessible to HSE employees and which are filtered (blocked). It covers the following areas:

- Filter internet content;
- Internet user access groups;
- Access to filtered internet content.

6.11 Service Provider Confidentiality Agreement

The *Service Provider Confidentiality Agreement* outlines the obligations of commercial third party service providers who are contracted by the HSE to provide data management services (i.e. data storage, hosting, application support, data transcription, data processing etc). It covers the following areas:

- How the service providers should handle HSE data;
- How the service provider should processed HSE data;
- How the service provider should store HSE data;
- Data Encryption;
- Data Transfer;
- International Data Transfers;
- The HSE's right to inspect and audit the service provider's data processing facilities.

6.12 Third Party Network Access Agreement

The *Third Party Network Access Agreement* outlines the specific terms and conditions governing the access and use of the Health Service Executive (HSE) network and information technology resources by a third party: It covers the following areas:

- Terms and conditions governing access;
- Default third party access privileges;
- Security of third party computer devices accessing the HSE network;
- Monitoring of third party access.

7.0 Roles & Responsibilities

7.1 Information Security Project Board (ISPB)

The ISPB Directorate is responsible for:

- Approving and publishing the policy;

- The annual review of policy;
- Approving all changes and amendments to the policy.

7.2 ICT Directorate

The ICT Directorate is responsible for:

- The identification, implementation and management of appropriate security controls necessary to safeguard the HSE's network (LAN/WAN) and supporting infrastructure;
- The implementation of system-level security controls as defined by the information owner or the CEO;
- The provision of facilities for information backups on network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;
- The provision of services which enable authorised user's access to appropriate electronic information systems and data;
- Liaising with and advising the HSE management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

7.3 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, contractors, sub-contractors, agency staff and third parties 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;

7.4 Line Managers

Line Managers are responsible for:

- The implementation of this policy and all other relevant 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 related HSE policies;

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

- Consulting with the Consumer Affairs section and the ICT Directorate in relation to the appropriate actions to be taken when an actual or suspected breach of data security has occurred.

7.5 Users

Each user 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;

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

- Reporting all actual or suspected breaches of data security to their line manager, the HSE Consumer Affairs section and their local ICT department immediately.

7.6 Internal Audit

Internal Audit are responsible for:

- Providing assurance that information technology controls and procedures are operated in accordance with the policies, regulations and best practice.

7.7 Consumer Affairs

Consumer Affairs are responsible for:

- Providing training and advice on data protection;

- Liaising with and advising the HSE management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

8.0 Policy Distribution & Awareness

- This policy and its supporting policies, standards and guidelines will be published on the HSE intranet. Hard copies of the policy and its supporting policies, standards and guidelines will be available on request from the local ICT departments.

- The ICT Directorate and/or the Information Security Project Board (ISPB) may make periodic policy announcements by email.

- HSE line managers will ensure that all existing and new staff, students contractors, subcontractors, agency staff and third party commercial service providers who report to them are made aware of and have access to the policy and its supporting policies, standards and guidelines.

- Data Protection training which also covers large sections of this policy and its supporting policies, standards and guidelines will be available from the HSE Consumer Affairs section.

- An *I.T. Security Policies Frequently Questions* booklet is available to download from the intranet. Further information and advice can also be accessed on the HSE Intranet website

- Individuals requiring clarification on any aspect of the policy and its supporting policies, standards and guidelines and/or advice on general I.T. security matters may email their queries to infosec@hse.ie address.

9.0 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.

- Updates to the policy and the supporting policies, standards and guidelines will be made periodically and will be posted on the HSE intranet and/or announced by email broadcast.

- The most up to date version of this policy is published on the HSE intranet

10 Breaches of Security

- For security and technical reasons the HSE reserves the right to monitor, record and log all use of its information technology resources and activity on the HSE network.

- Any individual suspecting that there has been, or is likely to be a breach of data security must inform their line manager, the Consumer Affairs section and their local ICT department immediately. The ICT department and Consumer Affairs will advise the individual and their line manager on what action should be taken.

- 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 procedures.

Appendix A

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

Availability: Ensuring that authorized users have access to information and associated assets whenever required.

Breach of Data Security: The situation where HSE confidential or restricted data has been put at risk of unauthorized disclosure as a result of the loss or theft of the data or, the loss or theft of a computer or storage device containing a copy of the data or through the accidental or deliberate release of the data.

Confidentiality: Ensuring that information is only accessible to those users who are authorized to access the information.

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

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

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.

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 region , directorate or service (i.e. HSE Regional Director of Operations (RDO), National Director **(**or equivalent)).

Information Security: The preservation of confidentiality, integrity and availability of information.

Information System: A computerized system or software application used to access, record, store, gather and process information.

Integrity: Ensuring the accuracy and completeness of information and associated processing methods.

Line manager: The individual a user reports directly to.

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.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

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.

Threat: A potential cause of an incident that may result in harm to a system or organisation.

Users: Any individual using any of the HSE's I.T. resources.