Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Access Control 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 Access Control Policy.
Purpose:	To define the correct use and management of system access controls within 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Superseded Documents:	All local Access Control Policies and Procedures.
Related Documents:	HSE Information Security Policy. HSE I.T. Acceptable Use Policy. HSE Password Standards Policy. HSE Remote Access Policy. Third Party Network Access Agreement. HSE Service Provider Confidentiality Agreement. HSE Information Classification & Handling Policy
Review Date:	February 2014
Contact Details:	Chris Meehan 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)	March 2010
2.0	HSE	Information Security Project Board (ISPB)	November 2010
3.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

The Health Service Executive (HSE) is legally required under the *Irish Data Protection Act 1988 & 2003* to ensure the security and confidentiality of the information it processes on behalf of its clients, patients and employees.

The HSE is committed to the correct use and management of access controls throughout the organization. Insufficient access controls or unmanaged access to information could lead to the unauthorized disclosure or theft of this information, fraud and possible litigation. The purpose of this policy is to define the correct use and management access controls within the 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 HSE information systems and network domains;
- 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 Access Control

- Where technically feasible all HSE Information Technology (I.T.) resources must be password protected.

- Each HSE information system must have a designated information owner who is responsible for managing and controlling access to the system. The information owner must hold a position within the HSE at national director level (or equivalent) and he/she must approve and sign all requests for access to the system. Alternatively the information owner may nominate a member(s) of their management team who will have the authority to sign and approve requests for access to the system on their behalf. Nominees in this regard must be at Grade 8 level (or equivalent) or higher. The information owner must forward the list of his/her nominees to the designated system administrator.

- Each HSE information system must have a designated system administrator(s) who is responsible for the day to day administration of the system including the creation and management of system access accounts for authorized users. Some information systems may for historical reasons be directly managed by the ICT Directorate and ICT personnel may perform the role of system administrator.

- The ICT Directorate is the designated owner of all HSE network domains. Each HSE network domain must have a designated network administrator(s) who is responsible for the day to day administration of the network domain including the creation and management of network domain access accounts for authorized users.

- Access to HSE information systems and networks must be strictly controlled by a formal written registration and de-registration process.

- Access to HSE information systems must be controlled by the use of individual user access accounts. The use of generic or group access accounts to access HSE Information Systems strictly prohibited.

- Access to HSE network domains will generally be controlled by the use of individual user access account’s, however the use of generic / group access accounts will be permitted on nominated computer devices that meet approved criteria (*see section 4.3.3*).

4.2 Account Privileges

- Access rights and privileges to HSE information systems and network domains must be allocated based on the specific requirement of a users HSE role / function rather than on their status

- The criteria used for granting access privileges must be based on the principle of “least privilege” whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their HSE role or function.
- Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.

- The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network. Each administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their standard user access account

4.3 Account Registration

4.3.1 Information System Access Accounts

- Access to HSE information Systems will be controlled by the use of individual user access accounts. The use of generic / group access accounts is not permitted under any circumstances on HSE information systems.

- All new requests for access to information systems must be made in writing using the ***HSE System Access Request Form*** *(http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Information_System_Access_Request_Form.pdf).*

- Line managers must complete the request on behalf of a new user and send this onto the designated information owner or his/her nominee for their approval. The request must be clearly marked '**New Access**'

- Information owners or their nominees must formally authorize and sign all new access requests. Once a request for access has been approved, the information owner or his/her nominee must sign the *HSE System Access Request Form* and forward this onto the system administrator for the user account to be created.

- System administrators must only create new user accounts when they have received a signed *HSE System Access Request Form.*

4.3.2 Network Domain Access Accounts

- Access to HSE network domains will generally be controlled by the use of individual user access account's, however the use of generic / group access accounts will be permitted on nominated computer devices that meet approved criteria. (*see section 4.3.3*)

- All new requests for access to a HSE network domain must be made in writing using the *HSE Network Domain Access Request Form* *(http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Information_System_Access_Request_Form.pdf).*

- Line managers (at Grade VIII level or higher) must complete the request on behalf of a new user and send this onto ICT Directorate. The request must be clearly marked **'New Access'.**

- Network administrators must only create new user accounts when they have received a signed *HSE Network Domain Access Request Form.*

4.3.3 Generic / Group Network Domain Access Accounts

- The use of generic / group access accounts is permitted on nominated computer devices that satisfy the following criteria:

    1) Computers need to remain logged onto the HSE network throughout the day to facilitate individual users gaining speedy access to clinical information systems using their own individual log on credentials (e.g. computers in a hospital A&E department)

    2) A single network computer is used by a number of different users throughout the day to facilitate access to clinical information systems using the users individual log on credentials (e.g. computers on a hospital ward)

- Where a generic / group access account is created on a HSE network domain, the generic / group access account must have an identified designated account owner (at grade 8 level (or equivalent) or above) who is responsible for the management and use of the generic / group access account.

- HSE network domain generic / group access accounts will only have access to an agreed set of HSE information systems and will not under any circumstances have access to HSE email or internet services**.** Limited network resources will be granted to a local named shared folder.

4.3.4 Third Party Access Accounts

- Where there is a business need and with the approval of a HSE information owner or his/her nominee third party commercial service providers maybe granted access to the HSE network and information systems.

- Third party commercial service provider access requests must be sponsored by a HSE information owner or his/her nominee and submitted to the ICT Directorate in writing using the *HSE Third Party Access Request Form* *(http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Third_Party_Access_Request_Form.pdf)*.

- The information owner or his/her nominee must complete the request on behalf of the third party and forward it to the ICT Directorate along with the following documents:

    1) A copy of the *HSE Third Party Network Access Agreement* signed by the third party commercial service provider (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Third_Party_Network_Access_Agreement.pdf*)

    2) A copy of the *HSE Service Provider Confidentiality Agreement* signed by the third party commercial service provider (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf*)

- Under no circumstances will third party commercial service providers be granted access to the HSE network and information systems until the ICT directorate has received the appropriate documentation.

- Third party commercial service provider access privileges will be agreed on a case by case basis. The third party commercial service provider must liaise with the HSE to establish the minimum privileges required by them in order for them to complete the service they have been contracted to perform.

- Local access (on-site) to the HSE network and information systems may be granted on a temporary basis only as and when the need arises. Remote access connections may be set up on a more permanent basis for ongoing information system or network support purposes.

4.3.5 Remote Access Accounts

- All remote access must be used and managed in accordance with the *HSE Remote Access Policy* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Remote_Access_Policy.pdf*).

4.4 Account Management

- Requests from users for password resets must only be performed once the user’s identity has been verified by the appropriate system administrator or network administrator (for example: a user’s identity maybe verified by the provision of their HSE personnel number).

- Existing user’s who require additional access privileges on an information system must obtain the written authorization of the designated information owner or his/her nominee. As per section **4.3.1** of this policy, line managers must initiate the requests using the *HSE System Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Information_System_Access_Request_Form.pdf*) and forward this to the designated information owner or his/her nominee. The request must be clearly marked '**Amend Current Access**' to avoid the creation of multiple accounts for the same user.

- Existing users who require additional access privileges on a network domain (for example file shares etc) must make their request in writing. As per section **4.3.2** of this policy, line managers must initiate the request using the *HSE Network Domain Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Information_System_Access_Request_Form.pdf*) and forward this to the ICT Directorate. The request must be clearly marked '**Amend Current Access**' to avoid the creation of multiple accounts for the same user.

- The access accounts of users taking career breaks, going on maternity leave or those on long term sick leave must be suspended until such a time as they return to work. Requests for account suspensions must be made in writing by the user's line manager using the *HSE Suspend / Remove Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Suspend_Remove_Access_Request_Form.pdf*) and forwarded to the ICT Directorate and the appropriate system administrator(s).The request should be clearly marked '**Suspend User Account**'.

- The access accounts of users who are about to change roles or transfer to another HSE directorate or service area, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed. In such circumstances the user's existing line manager must request the removal of the unnecessary account privileges. The request must be made in writing using the *HSE Suspend / Remove Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Suspend_Remove_Access_Request_Form.pdf*) and forwarded to the ICT Directorate or the appropriate system administrator before the user changes role or transfers. The request should be clearly marked '**Removal of User Account Privileges'**.

4.5 Account De-Registration

- As soon as a user leaves the employment of the HSE all his/her information systems and network access accounts must be revoked immediately. Line managers must request the deletion of a user's access accounts as soon as they have been informed by the user that they are leaving the employment of the HSE. The requests must be made in writing using the *HSE Suspend / Remove Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Suspend_Remove_Access_Request_Form.pdf*) and forwarded to the ICT Directorate and the appropriate system administrator(s). The request should be clearly marked **'Delete User Account'** and made in advance of the users last day.

- System administrators and network administrators must revoke user accounts at the requested date and time after the receipt of a properly completed *HSE Suspend / Remove Access Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Suspend_Remove_Access_Request_Form.pdf*).

4.6 Security

- Access to all information systems and networks must be controlled via strong password authentication schemes.

- User access accounts must be created in such a way that the identity of each user can be established at all times during their usage. Each user access account must be unique and consist of at least a user name and password set. All passwords created must be inline with the requirement 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).*

- Where possible HSE information systems and networks must be configured to:

    1) Force users to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password, the first time they logon to a HSE information system or network.

    2) Automatically 'lock' a user account after a number of consecutive failed login attempts.

    3) Automatically 'lock' or log out user accounts after 30 minutes of inactivity. Where this is not possible, users must be instructed to manually log off or 'lock' their HSE computer device (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time and at the end of the each working day.

- When available audit logging and reporting must be enabled on all information systems and networks.

4.7 Monitoring & Review

- Information owners or their nominees must continually monitor access to their information systems. They must perform quarterly reviews of the systems they are responsible for to ensure:

    1) That each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function;

    2) That the information system and the information processed by the system is only accessed and used by authorized users for legitimate reasons.

- System administrators and network administrators must conduct a system/network domain review at least once every quarter. User access accounts which have been inactive for 60 consecutive days or more must be suspended unless instructed otherwise by the user's line manager. Suspended user accounts which have <u>not</u> been reactivated within a 12 month period should be marked for deletion, unless instructed otherwise by the user's line manager.

5.0 Roles & Responsibilities

5.1 Information Owner

Each designated information owner is 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;

- Ensuring adequate backup procedures are in place for the information system they are responsible for;

- Ensuring all access requests are evaluated based on the approved criteria;

- Sponsoring and approving third party access requests (locally or remotely) to the HSE information system they are responsible for;

- Designating system administrator(s) for the information system they are responsible for;

- Furnishing the system administrator with a list of nominees who are authorised to approve and sign access requests to the information system on their behalf;

- Conducting a quarterly review of the information system in accordance with this policy;

- Informing the ICT Directorate & Consumer Affairs immediately in the event of a security incident involving the systems they are responsible for.

5.2 System Administrator

Each system administrator is responsible for:

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

- Taking appropriate and prompt action on receipt of requests for user registration, change of privileges, password resets and de-registration of users in accordance with this policy and the procedures for the information system;

- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the information system;

- Ensuring all passwords generated for new user accounts and password resets 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);*

- Notifying users of their system account details in a secure and confidential manner;

- Ensuring that appropriate records of system activity, including all authorized user registrations, change of privileges and de- registration requests are maintained and made available for review to the appropriate personnel;

- Conducting a quarterly review of the information system they re responsible in accordance with this policy;

- Notifying the designated information owner, if they suspect a user is responsible for misusing the information system or is in breach of this policy;

- Informing the designated information owner immediately in the event of a security incident involving the system;

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

5.3 Network Administrator

Each network administrator is responsible for:

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

- Taking appropriate and prompt action on receipt of requests for user registration, change of 'privileges', password resets and de-registration of users in accordance with this policy and the procedures for the network;

- Taking appropriate and prompt action on receipt of requests for the suspension of a user account in accordance with this policy and the procedures for the network;

- Ensuring all passwords generated for new user accounts and password resets 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);*

- Notifying users of their system account details in a secure and confidential manner;

- Ensuring that appropriate records of system activity, including all authorized user registrations, change of 'privileges' and de- registration requests are maintained and made available for review to the appropriate personnel;

- Conducting a quarterly review of the network they re responsible in accordance with this policy;

- Notifying a users line manager, if they suspect the user is responsible for misusing the network or is in breach of this policy;

- Informing the ICT Information Security Unit immediately in the event of a security incident involving the system.

5.4 ICT Directorate

The ICT Directorate is responsible for:

- The management, control, ownership, security and integrity of all HSE network domain (LAN/WAN) on behalf of the HSE;

- The implementation of this policy and all other relevant policies within the ICT Directorate;

- Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies;

- Designating a network administrator(s) for each HSE network domain;

- Conducting a quarterly review of the networks in accordance with this policy;

- Providing information owners or their nominees with quarterly audit reports and user access lists for information systems which are directly managed by the ICT Directorate.

5.5 Line Managers

Each Line Manager is 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 members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant HSE policies;

- Ensuring complete and timely user access requests, for both permanent and temporary staff, are forwarded to the designated system owner allowing sufficient time for the creation of the required user account prior to the users start date;

- Ensuring complete and timely user network access requests, for both permanent and temporary staff, are forwarded to the ICT Directorate allowing sufficient time for the creation of the required user account prior to the users start date;

- Ensuring that each user they request access fulfills all the criteria (principle of "least privilege") for the requested information system and/or network;

- Ensuring they make timely requests for the suspension of all user accounts belonging to members of their staff who are taking a career break, going on maternity leave or leave or those on long term sick leave;

- Ensuring they make timely requests for the deletion of all user accounts belonging to members of their staff who are leaving the employment of the HSE;

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

5.6 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 systems and network they access, and the information processed by those systems or networks;

- Ensuring they only use user access accounts and passwords which have been assigned to them;

- Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties;

- Changing their passwords at least every 90 days or when instructed to do so by designated system administrators, network administrators or the ICT Directorate;

- Complying with instructions issued by designated information owners, system administrators, network administrators and/or the ICT Directorate on behalf of the HSE;

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

6.0 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.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary to ensure 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 at – (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/)

Appendix A

Access: All local or remote access to the HSE network and information systems.

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

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.

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

Generic / Group Access Account: An access account that is intended for use by a number of different people and not an individual user and as such is not derived from a single user’s name.

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

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 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.

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

Line manager: The individual a user reports directly to.

Network Administrators: These are the individuals responsible for the day to day management of a HSE network domain. Also includes HSE personnel who have been authorised to create and manage user accounts and passwords on a HSE network domain.

Network Domain: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules

Personal Information: Information relating to a living individual (i.e. HSE employee, client or 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.

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

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.

Remote Access: Any Connection to the HSE network(s) or information systems that originates from a computer or device located outside of the HSE network.

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 restricted 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

System Administrator: The individual(s) charged by the designated system owner with the day to day management of HSE information systems. Also includes the HSE personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

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.

Users: Any authorized individual using any of the HSE's IT resources.