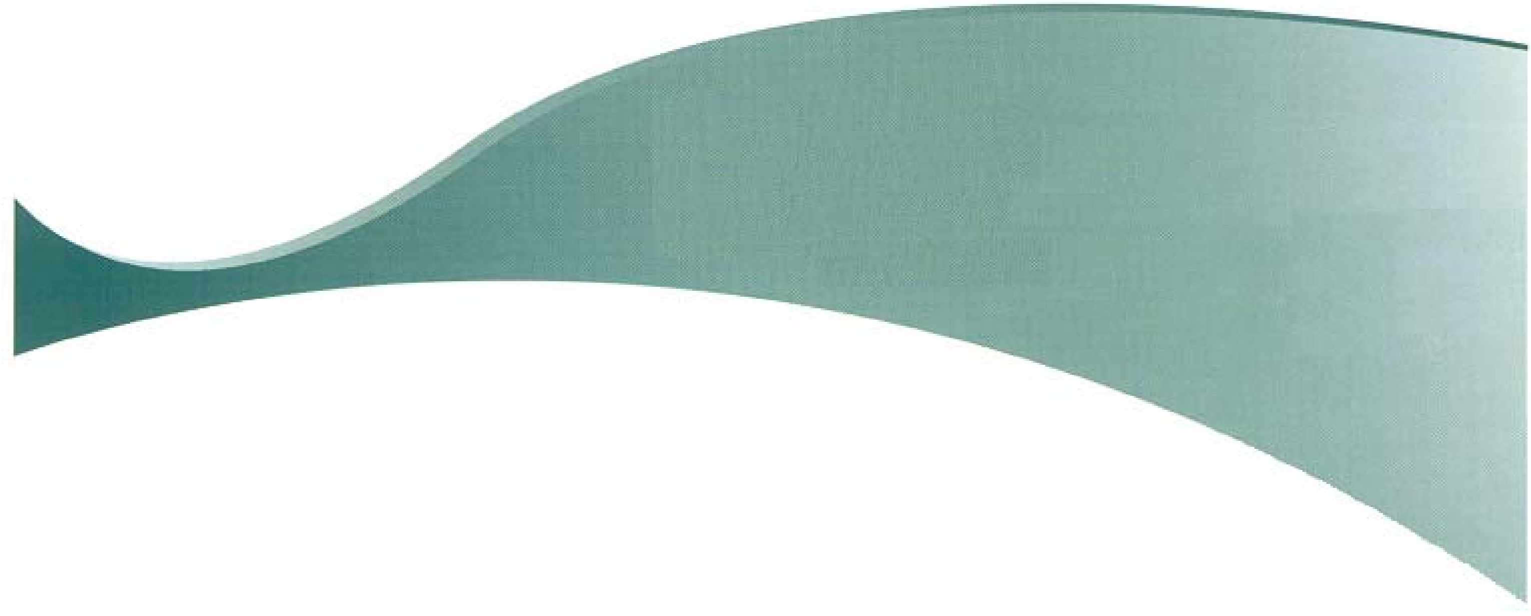
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

# *Password Standards 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 Password Standards Policy. |
| **Purpose:** | To provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change. |
| **Author:** | Information Security Project Board (ISPB) on behalf of the HSE. |
| **Publication date:** | February 2013 |
| **Target Audience:** | All system developers and 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| **Superseded Documents:** | All local password standard policies and procedures. |
| **Related Documents:** | HSE Information Security Policy.<br>HSE Information Technology Acceptable Use Policy.<br>HSE Electronic Communications Policy.<br>HSE Encryption Policy. |
| **Review Date:** | February 2014 |
| **Contact Details:** | Chris Meehan<br>ISPB Secretary,<br>ICT Directorate<br>Dr.Steevens Hospital<br>Steevens Lane<br>Dublin 8<br>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

Passwords are one of the primary mechanisms that protect critical HSE information systems and other resources from unauthorised use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and protection could allow unauthorised access to the HSE's Information Technology (I.T.) resources, which in turn could lead to the inappropriate disclosure and use of confidential or sensitive HSE information. The purpose of this policy is provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change.

This policy is mandatory and by accessing any 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 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 HSE Information Technology (I.T.) equipment, systems and applications which are capable of being password protected;

- All system developers and 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 Password Security

- Where technically feasible all HSE Information Technology (I.T.) resources must be protected by the use of strong passwords.

- All passwords created for use within the HSE must meet the requirements of this policy.

### 4.2 Monitoring & Auditing

The ICT Directorate on behalf of the HSE reserves the right to monitor and audit all password use within the HSE to ensure compliance with this policy and to identify any weak passwords that could compromise the security of Information Technology (I.T.) equipment, systems, applications or the network.

### 4.3 Password Standard

- All passwords must be unique and meet the following standard:

#### 4.3.1 Password Length

- All passwords must be a minimum of 8 characters in length. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed within the system must be used.

#### 4.3.2 Password Complexity

- Passwords <u>must contain</u> a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €).

- Passwords <u>must not</u> be left blank.

- Passwords or part of a password <u>must not</u> contain:

    1) Any word(s) found in an English or foreign language dictionary;

    2) Any word(s) spelled backwards - (for example: drow, yadnom);

    3) Any slang words - (for example: dubs, agro, bling);

    4) Any word with numbers appended (for example: deer2000, password2012, Paul2468 etc);

    5) Any words with simple obfuscation (for example: p@ssw0rd, l33th4x0r, @dm1n100, g0ldf1sh, etc);

    6) Any names of fictional characters - (for example: frodo, shrek );
    7) Any common keyboard sequences - (for example: qwerty);

8) Any names of people, places or organisations - (for example: mary100, Liverpool, LFC2005, ManUtd);

9) Any personal information related to a user - (for example: user name, address, date of birth, HSE personnel number, car registration number, telephone number);

10) A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);

11) The following sequence of letters - passwrd, passwd, pwrd, paswd, passwd.

- Guidance and help on creating secure passwords can found on the intranet at (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Security_and_Standards/Security/Security_Awareness/Password_security/Creating_Strong_Passwords.html*).

### 4.3.3 Password History

- No password may be re-used by a user within a 12 month period.

### 4.3.4 Password Aging

- User-level passwords such as those used to access HSE computer devices, information systems and network domains must be changed at least every 120 days.

- System-level passwords such as those used by HSE information system administrators and network domain administrators must be changed at least every 90 days.

## 4.4 Password security

- Users should avoid using the same password for multiple system or purposes.

- Each user is responsible for all activities performed on any HSE I.T. device, information system or application while logged in under their individual access account and password.

- With the exception of generic / group access accounts users must only use user access accounts and passwords which have been assigned to them.

- Users must ensure all passwords except those used for generic / group access accounts are kept confidential at all times and are not shared with others including their co-workers or third parties.

- Users must not write down their password(s) on or near their computer device. However in exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

- Users must not send their passwords within email messages unless the email message is encrypted.

- Users must change their passwords at least every 120 days or when instructed.

- Users who suspect their password is known by others must change their password immediately.

- Users must not misuse their own or another users password and knowingly elevate their information system access account or network domain access privileges above those that they have been authorized to use.

- User must ensure all default passwords which are supplied by a vendor for new HSE devices and systems are changed at installation time.

## 4.5 System & Application Development Standards

- System developers (including both HSE personnel and third party commercial service providers) who are responsible for developing information systems and applications for the HSE or its customers must ensure that the systems and applications they develop are capable of implementing, supporting and enforcing this policy in full.

- System developers (including both HSE personnel and third party commercial service providers) who are responsible for developing information systems and applications for the HSE or its customers must ensure that the systems and applications they develop contain the minimum security features:

  1) They must support authentication of individual users and not just groups;

  2) They must contain controls that can ensure that individuals can be held responsible for their actions;

  3) They must not store passwords in clear text or in any easily reversible form;

4) The password should not be displayed on the screen when they are being entered;

5) They must provide for some sort of role management, such that one user can take control of the functions of another without having to know the other users password;

6) They must force users to change their password at their first logon.

7) They must automatically 'lock' a user account after a defined number consecutive failed login attempts.

8) They automatically 'lock' or log out user accounts after a defined period of inactivity.

9) They must provide a logging facility that as a minimum is capable of recording all failed and successful login attempts;

10) They should support TACACS+, RADIUS and/or X.509 with LDAP security retrival, wherever possible.

## 5.0 Roles & Responsibilities

### 5.1 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;

### 5.2 Network Domain Administrators

Each HSE network administrator is responsible for:

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

- Ensuring all passwords generated for new user accounts and password resets meet the requirements of this policy;

- Notifying users of their passwords in a secure and confidential manner.

### 5.3 System Administrators

Each HSE system administrator is responsible for:

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

- Ensuring all passwords generated for new user accounts and password resets meet the requirements of this policy;

- Notifying users of their passwords in a secure and confidential manner;

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

### 5.4 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 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 120 days or when instructed to do so by designated system administrators, network domain 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.

### 5.5 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.

### 5.6 System Developers

In addition to the above system developers (including both HSE personnel and third party commercial service providers) are responsible for:

- Ensuring the systems and applications they develop for the HSE are capable of implementing, supporting and enforcing this policy in full.

## 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 IT 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 organization structure and business practices are properly reflected in the policy.

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

# Appendix A

**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.

**Line manager**: The individual a user reports directly to.

**Network Domain Administrators:** 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.

**Password:** A string of characters that a user must supply in order to gain access to an IT resource.

**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.

**System Administrators:** 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.

**System Developer**: Any HSE personnel or third party commercial service providers who are responsible for developing electronic information systems and application for the HSE or its customers.

**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 who uses the HSE's I.T. resources.