Please 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/
**Title:** Data Protection Breach Management Policy

**Purpose:** To outline the approved HSE management approach to be followed in the event of data protection breach.

**Author:** Consumer Affairs Directorate on behalf of the HSE.

**Publication date:** February 2010

**Target Audience:** All HSE employees, service providers, clients and third parties that have access to the HSE’s information

**Superseded Documents:** All local breach management policies.

**Review Date:** February 2011

**Contact Details:**
Mr Ray Mitchell,  
Parliamentary and Regulatory Affairs,  
Health Service Executive,  
Park Gate St Business Centre  
Park Gate St  
Dublin,  
Tel No : 01 6352503  
ray.mitchell@hse.ie
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/data it processes on behalf of its clients, patients and employees.

Information/data 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/data is essential to the successful operation of the HSE in the provision of services to our patients and clients.

Sometimes a breach of information/data security may occur because this information/data is accidentally disclosed to unauthorized persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device.

The purpose of this policy is to ensure that a national standardised management approach is implemented throughout the organisation in the event of an information/data breach.

This policy is mandatory and by accessing any of the HSE’s Information/data, 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 may have been developed at a local level. The policy applies to all HSE employees, service providers, contractors and third parties that access, use, store or process information on behalf of the HSE. This policy is authorised by the Senior Management 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:

- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)
4.0 Policy

It is the policy of the HSE that in the event that an information/data breach happens, the following breach management plan is strictly adhered to.

It is important that each HSE Directorate puts into place their own local procedures to enable them to implement the breach management plan should such a data breach occur. There are five elements to any breach management plan:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

5.0 Breach Management Plan

5.1 Identification and Classification

Directorates must put in place procedures that will allow any staff member to report any information/data security breach.

- It is important that all staff are aware to whom they should report such a breach.

- Having such a procedure in place will allow for early recognition of the breach so that it can be dealt with in the most appropriate manner.

- Details of the breach should be recorded accurately, including the date and time the breach occurred, the date and time it was detected, who/what reported the breach, description of the breach, details of any ICT systems involved, corroborating material such as error messages, log files, etc.

- In this respect, staff need to be made fully aware as to what constitutes a breach. In respect of this policy a breach maybe defined as the unintentional release of HSE confidential or personal information/data to unauthorised persons, either through the accidental disclosure, loss or theft of the information/data.

5.2 Containment and Recovery

Containment involves limiting the scope and impact of the breach of data/information. If a breach occurs, Directorates should:

- Decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation.

- Establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment
exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.

- Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause.

### 5.3 Risk Assessment

In assessing the risk arising from the security breach, Directorates should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Directorates should consider the following points:

- What type of Information/data is involved?
- How sensitive is the information/data?
- Are there any security mechanism’s in place (e.g. password, protected, encryption)?
- What could the information/data tell a third party about the individual?
- How many individuals’ are affected by the breach?

### 5.4 Notification of Breaches

- All information/data breaches must be reported to the Consumer Affairs or ICT Directorate immediately. Members of staff and their line manager must complete a **Data Breach Incident Report** and forward (via fax or email a scanned copy) this to their local Consumer Affairs Officer for breaches involving manual (paper based) information/data or the their local ICT call centre/helpdesk for breaches involving electronic data.

- Under no circumstances should directorates inform the Data Protection Commissioners Office directly. The Local Consumer Affairs Officer will notify the Data Protection Commissioners office of the breach if required.

- Directorates should consider notifying third parties such as the Garda if necessary.

### 5.5 Evaluation and Response

- Subsequent to any information/data security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.
• Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

• Each Directorate should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

6.0 Roles and Responsibilities

6.1 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 Consumer Affairs &/or the ICT Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

6.2 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;

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

7.0 Enforcement

The HSE reserves the right to take such action as it deems appropriate against users who breach the conditions of this policy. HSE employees who breach this policy may be denied access to the organization’s information technology resources, and may be subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.

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.