NATIONAL SHARED SERVICES OFFICE (NSSO)

DATA SECURITY BREACH INCIDENT MANAGEMENT POLICY

Change History

Document Name	Data Security Breach Incident Mgmt. Policy
Date Created	24/05/2018
Document Owner	NSSO Information Governance Team – AP Gráinne NicDhonnacha

Version Control

Date of Edit	Version No. (after edit)	Editor	Description of Change e.g. page no. /Summary of changes made.
24/05/2018	V1	HRSS IGT	Policy Created

Contents

1. Purpose

The purpose of this policy is to ensure that a standardised approach is implemented throughout the organisation in the event of an information/data breach. This policy is mandatory and by accessing any of the National Shared Services Office's (NSSO) information/data, users are agreeing to abide by the terms of this policy.

2. Scope

This policy represents the NSSO's position and takes precedence over all other relevant policies which may have been developed. The policy applies to all NSSO employees, service providers, contractors and third parties that access, use, store or process information on behalf of the NSSO. This policy is authorised by the Senior Management of the NSSO.

3. Legislation

The NSSO has an obligation to abide by all relevant Irish Legislation and European Legislation.

4. Policy

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

5. Breach Management Plan

There are five elements to any breach management plan:

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

6. Identification and Classification

The NSSO must have procedures in place that will allow any staff member to report an information/data security breach. It is important that all staff are aware to whom they should report such a breach – please see contact details at Appendix 1.

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 the breach occurred, the date it was detected, who reported the breach, description of the breach, etc., - please see Appendix 2 "**Data Breach Report and Corrective and Preventive Action (CAPA) Form**".

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 unauthorised release of confidential or personal information/data held by the NSSO, to unauthorised persons, either through accidental disclosure, loss or theft.

7. Containment and Recovery

Containment involves limiting the impact of the breach of data/information. If a breach occurs, NSSO staff must immediately:

- Inform the appropriate NSSO Data Protection Team:
  - HR Shared Services: dataprotection@peoplepoint.ie
  - Payroll Shared Services: dataprotection@pssc.gov.ie
  - Financial Shared Services: [1]To be provided.
  - NSSO HR: nssoresourcing@nsso.gov.ie
- CC the Data Protection Officer (see Appendix 1) on the above email
- Secure the Data
- Complete the CAPA Form.

8. Risk Assessment

In assessing the risk arising from the security breach, the NSSO Data Protection Team must consider what would be the level of risk to the data subjects affected 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, the Data Protection Team should consider the following points:

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

[1] The Financial Shared Services is currently in project phase. Contact details will be provided once the division is operational, upon project completion.

9. Notification of Breaches

All information/data breaches must be reported to the Data Protection Team immediately. Members of staff and their line manager must complete the official NSSO Data Breach Report and Corrective and Preventive Action (CAPA) Form (See Appendix 2) and forward the completed document by email to the appropriate Data Protection Team:

Payroll Shared Services: dataprotection@pssc.gov.ie
HR Shared Services: dataprotection@peoplepoint.ie
Finance Shared Services: To be provided.

10. Evaluation and Response

Following any data security breach a thorough review and root cause analysis of the incident will 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.

11. Roles and Responsibilities

Line Managers

Line Managers are responsible for:

- The implementation of this policy within their areas of responsibility.
- Ensuring that all NSSO employees who report to them are made aware of and are instructed to comply with this policy.
- Consulting with the NSSO Data Protection Team in relation to the appropriate procedures to follow when a breach has occurred.

NSSO Staff

Each staff member is responsible for:

- Complying with the terms of this policy.
- 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.

12. Policy Review

This policy will be reviewed and updated periodically to ensure that any changes to the NSSO's structure and business practices are properly reflected in the policy.

Appendix 1

Contact details for the NSSO Data Protection Officer

Adam Egan
Data Protection Officer
National Shared Services Office
Leeson Lane
Dublin 2
D02 TR60

Email: DPO@nsso.gov.ie
Phone Number: 086 701 3294

Appendix 2

Data Breach Report and CAPA Form
(Internal Record-To be completed by Manager and Officer)

Data Breach Details:

Relevant Case ID's:		Functional Team where Data Breach occurred:	Choose an item.
Date Data Breach occurred:	Click here to enter a date.	Date HRSS was informed of Data Breach:	Click here to enter a date.

To be completed by officer & line manager:

Containment Has data been contained? (Request for deletion/retrieval of document/data shared):	Choose an item.	If 'no' please provide reason why data has not been secured:	
Data Controller Department where the data subject (individual whose data was breached) is employed:	Choose an item.	How was Data Breach identified (please provide name of individual if possible):	

Type of Data Breach:	Choose an item.	If 'Other' please give details:	
Personal Data Nature of the data breached (state each unit personal data-PPSN, Name, Email etc.):			
Root Cause Analysis Outline details of data breach-what happened and also how the Data Breach occurred (Please state exactly **how or why** the error occurred):			
Data Subjects No. of individuals whose data was affected in this breach:			

To be completed by line manager:

Corrective/Preventative Action Outline all corrective and preventative measures taken to eliminate further risk of the occurrence of the same type of data breach:	Choose an item.	If 'Other' please give details	