SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

SETU Data Breach Reporting Form

The Data Breach Reporting Form consists of three sections designed to ensure a full audit trail and record of the data breach and follow up is maintained.

Section A: Initial Incident Report
Section B: Investigation, Assessment and Response
Section C: Post Incident Review

Section A: Initial Incident Report

To be completed by the individual reporting the incident and/or the appropriate Head of Faculty/Head of Function/Head of Department. Students or external 3rd parties should complete the form and provide it to the appropriate Head of Faculty/ Head of Function/Head of Department.

Name:	**Function:**
Date:	**Time of Incident:**
Date of Incident:	**Time of Notification:**
Who was Notified?	
Description of Incident: (e.g. impacted systems, witnesses to the incident, websites etc.)	
Type of breach: (confidentiality breach, availability breach, integrity breach)	
Specific details of the breach (What happened? Which systems/files affected? Who was involved? Categories of data affected? How did this occur?)	

Comments

Section B: Investigation, Assessment and Response

To be completed by the appropriate Head of Faculty/Head of Function/Head of Department

Estimated number of data subjects affected:	**Estimated number of records affected:**

Categories of data subject affected: (e.g. employees, students, the public, suppliers etc.)

Categories of personal data affected: (e.g. Contact Details, Health Data, Bank Details, etc.)

Potential risks to the data subject/likely consequences of the personal data breach: (see notes on page 4)

Mitigating factors in place or proposed to be actioned:

Assessment of likelihood of risks to data subject:

Assessment of severity of risks to the data subject:

Likely to result in a risk to the rights and freedoms of the data subject? (Y/N and justification).
Note: If yes it should be reported to the Data Protection Commission. Please contact the Data Protection Officer to report – dpo@setu.ie

***Risk Level? (None, Low Risk, Medium Risk, High Risk, Severe Risk and include justification). Note: If some level of risk report to Data Subject –** See page 4 for risk rating definitions.

Comments

Signed By:

Date:

Section C: Post Incident Review

To be completed by the appropriate Head of Faculty/Head of Function/Head of Department and reviewed by the Data Protection Officer)

Potential weaknesses identified which are required to be remediated?

What action have you taken to prevent similar incidents in the future?

Has there been any media coverage of the incident?

Is a Data Protection Impact Assessment ('DPIA') required for the process in light of new information?

Has SETU communicated the breach to the Data Protection Commission and Data Subject where necessary? If so, please provide their details and an outline of their response.

Comments	
Signed by Manager:	**Date:**
Signed by DPO:	**Date:**

Notes

***Self- Declared Risk Rating**

In determining how serious you consider the breach to be for affected individuals, you should take into account the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact you should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place, and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below:

- **Low Risk:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- **Medium Risk:** The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- **High Risk:** The breach may have a considerable impact on affected individuals.
- **Severe Risk:** The breach may have a critical, extensive or dangerous impact on affected individuals.