SETU Data Breach Reporting Form

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:	**Staff Number:**
Date of Incident:	**Time of Incident:**
Who was Notified?	**Time of Notification:**

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, 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:	
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, medium, high and include justification). Note: If some level of risk report to Data Subject	
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?
Have we recorded communications 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 **Staff Manager:**	**Date:**