PERSONAL DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your Head of Department/Office immediately. Heads of Department/Office to complete Section 1 of this form and email it to the Information Compliance Manager at foi@ucc.ie

Section 1: Notification of Data Security Breach	To be completed by Head of Dept/School/Office of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number, UCC address):	
Brief description of incident or details of the information lost:	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	

For University use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by Information Compliance Manager in consultation with head of area affected by the breach
Details of information loss:	
If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
Is the data bound by any contractual security arrangements e.g. to research sponsors?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data ○ **Special Categories of personal data** relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) membership of a trade union; e) genetic or biometric data; f) data concerning health; g) data concerning a person's sex life or sexual orientation; Also consider data relating to criminal convictions/offences as sensitive.	
○ Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;	
○ Personal information relating to vulnerable adults and children;	
○ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
○ Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
○ Security information that would compromise the safety of individuals if disclosed.	
Category of incident (1, 2a, 2b or 3):	
If level 2b or level 3, date escalated by Corporate Secretary to the University's Emergency Management Team (EMT)	

Section 3: Action taken	To be completed by Information Compliance Manager
If notified to Data Protection Commission, provide details, incl. date:	
If notified to data subjects, provide details, incl. date:	
If notified to other external, regulator/stakeholder, provide details:	
If reported to Gardai, provide details, incl. dates:	
If notified to other internal stakeholders, provide details and dates:	
Follow up action required/recommended:	