**Information Security Incident Management Policy**

# Purpose and scope

The purpose of this policy is to ensure a consistent and effective approach to the management of Information Security Incidents, provides a definition of an Information Security Incident and establishes a structure for the reporting and management of such incidents. This policy supports the university in demonstrating its compliance with data protection legislation, which primarily includes the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), to data subjects and the regulator for data protection and privacy in the UK (Information Commissioner).

This policy applies to members of Cardiff University as defined under Ordinance 2 – Members of the University and any other party engaged where personal data is processed on behalf of Cardiff University.

# Policy

Cardiff University shall at all times address information security incidents efficiently and effectively and ensure that they are managed in accordance with the Information Security Incident Reporting and Management Procedure

All members of the university shall be made aware of the procedure for reporting Information Security Incidents and their responsibility to report such incidents.

The severity of the incident shall be assessed and the management response shall be proportionate to the threat, invoking the Major Incident Plan where appropriate, to minimise the risks and adverse impact on any interested party. Relevant staff shall be trained in digital evidence collection, retention, recovery and presentation in accordance with legislative or regulatory obligations.

New risks identified as a result of an incident shall be assigned to the relevant risk owner and acceptable risks shall be mitigated promptly in accordance with the university’s risk management processes and in accordance with the Information Security Incident Reporting and Management Procedure.

Key information about information security incidents, including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analysed in order to assess the effectiveness of information security controls.

New risks identified as a result of an incident shall be assigned to the relevant risk owner and unacceptable risks shall be mitigated promptly in accordance with the university’s risk management processes and in accordance with the Information Security Incident Reporting and Management Procedure.

An Information Security Incident is the occurrence or development of an unwanted or unexpected situation which indicates either:

1. a possible breach of an information security framework policy or
2. a failure of information security controls which have a significant probability of compromising business operations.

This definition covers action or omission by Cardiff University members and any of its sub-contractors that process the university’s Classified information. Examples of Information Security Incidents include (but are not limited to):

* Accidental or unauthorised disclosure of Classified C1 ‘Highly Confidential’ or C2 ‘Confidential’ information including personal data (e.g. via misaddressed correspondence, incorrect attachment to record or incorrect system access permissions/filter failure)
* Direct loss or theft of Classified C1/C2 information (e.g. papers taken from car, post intercepted, unauthorised download)
* Loss or theft of equipment used to store Classified Information C1/C2 (e.g. laptop, smartphone, USB stick)
* Corruption or unauthorised modification of vital records (e.g. alteration of master records)
* Computer system or equipment compromise (e.g. virus, malware, denial of service attack)
* Compromised IT user account (e.g. spoofing, hacking, shared password)
* Break in at a location holding Classified information or containing critical information processing equipment such as servers

Information security incidents shall be escalated according to the risk management criteria within the Information Security Incident Reporting and Management Procedure and reported to the appropriate external authorities where relevant by authorised individuals.

# Roles and Responsibilities

All members of the university are responsible for reporting actual or suspected Information Security Incidents directlyto the IT Service Deskwithout undue delay in accordance with the Information Security Incident Reporting and Management Procedure. Local procedures which conflict with this are not permitted.

Failure to report an Information Security Incident and any other breach of this policy shall be considered to be a disciplinary matter and shall be reported to the Senior Information Risk Owner for onward transmission to HR in order that it can be addressed under the relevant disciplinary/conduct procedure.

Contractors (including their agents and sub-contractors) undertaking work on the university’s information systems and services shall be required to note and report any significant information security weaknesses in those systems or services.

The responsibility for responding to information security incidents shall be as set out in the Information Security Incident Reporting andManagement Procedure.

The responsibility for reporting serious Information Security Incidents to external authorities lies with the Senior Information Risk Owner unless otherwise delegated in the Information Security Incident Reporting andManagement Procedure.

Heads of School/Director of Professional Service shall be responsible for monitoring their department’s compliance with the university Information Security Incident Management Policy.

# Related policies and procedures

This policy forms part of the Information Security Framework. It should also be read in conjunction with**:**

* the Information Security Incident Reporting and Management Procedure
* the Managing and Reporting Concerns appendix of the Safeguarding Vulnerable Adults and Children Policy
* Card Payment Data Security Policy and Procedure

**Version control table**

|  |  |  |
| --- | --- | --- |
| Document Name | Information Security Incident Management Policy | |
| UEB Policy Sponsor | Senior Information Risk Owner – University Secretary and General Counsel | |
| Policy Owner | Senior Compliance Advisor & Data Protection Officer, University Secretary’s Office | |
| Policy Author(s) | Senior Compliance Advisor & Data Protection Officer, University Secretary’s Office | |
| Version Number | 1.1 | |
| Equality Impact Outcome and Form Submission Date |  |  |
| Approval Date | June 2023 | |
| Approved By | Senior Information Risk Owner | |
| Date of Implementation | July 2023 | |
| Date of Last Review | April 2018 | |
| Date for Next Review | July 2024 | |
| For Office Use – Keywords for search function |  | |