Information Security Incident Management Policy

Version Number:	1.0
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Data and Information Management Oversight Group
Effective Date:	19 April 2018
Date of Next Review:	March 2020

1 Purpose

The purpose of this policy is to ensure a consistent and effective approach to the management of Information Security Incidents, including communication on security events and weaknesses. It enables the efficient and effective management of Information Security Incidents by providing a definition of an Information Security Incident and establishing a structure for the reporting and management of such incidents.

2 Scope

This policy applies to all members of the University with reference to all information held by or on behalf of the University. For the definition of an Information Security Incident see 'Definitions' section below.

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should also be read in conjunction with the Managing and Reporting Concerns appendix of the Safeguarding Vulnerable Adults and Children Policy.

4 Policy Statement

Information Security Incidents shall be reported promptly and responded to in a quick, effective and orderly manner in order to reduce the negative effect of incidents, to repair damage and to inform policy and mitigate future risks.

5 Policy

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

5.2 All Information Security Incidents shall be reported promptly to the IT Service Desk in accordance with the Information Security Incident Reporting Procedure.

5.3 All Information Security Incidents shall be managed in accordance with the Information Security Incident Management Response Procedure. The severity of the incident shall be assessed and the management response shall be proportionate to the threat.

5.4 Key information about serious 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.

5.5 New risks identified as a result of an incident and shall be assigned to the relevant risk owner and unacceptable risks shall be mitigated promptly in accordance with the University's risk management processes.

5.6 Relevant staff shall be trained in digital evidence collection, retention, and presentation, in accordance with legislative or regulatory obligations.

5.7 Serious incidents shall be reported to the appropriate external authorities where relevant by authorised individuals.

6 Responsibilities

6.1 All members of the University are responsible for reporting actual or suspected Information Security Incidents to the relevant internal contact as soon as possible in accordance with the Information Security Incident Reporting Procedure

6.2 Contractors using the University's information systems and services shall be required to note and report any significant information security weaknesses in those systems or services.

6. 3 The responsibility for responding to Information Security Incidents shall be as set out in the Information Security Incident Management Procedure.

6.4 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 Management Procedure.

7 Compliance

7.1 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 to be addressed under the relevant disciplinary code.

7.2 Compliance with this policy should form part of any contract with a third party that may involve access to University networks, computer systems or data. Failure by contractors to comply with clause 6.2 of this policy may constitute an actionable breach of contract.

8 Definitions

Information Security Incident

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

a) a possible breach of an information security framework policy **or**

b) a failure of information security controls which have a significant probability of compromising business operations.

Examples of Information Security Incidents include (but are not limited to):

- Direct loss or theft of Classified Information (e.g. papers taken from car, post intercepted, unauthorised download)
- Loss or theft of equipment used to store Classified Information (e.g. laptop, smartphone, USB stick)
- Accidental or unauthorised disclosure of 'Confidential' or 'Highly Confidential' Classified Information (e.g. via misaddressed correspondence or incorrect system permissions/filter failure)
- 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

A *serious Information Security Incident* is an incident whose impact, if unmanaged, has the potential to reach Moderate or above on the University's Risk Measurement Criteria. Incidents involving images of child sexual abuse will always be categorised as serious.

Classified Information is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature. Further explanations of these classifications can be found in the University's Information Classification document