Baseline University Expectation

Information Security Incident Management Policy Summary

a) **What is Information Security Incident Management?**
Information security incident management ensures a consistent approach to the management of information security incidents, including communication on security events and weaknesses.

Information security incidents are defined as the occurrence or development of an unwanted or unexpected situation which indicates **either**:

1) a breach, threat, weakness, or malfunction that impacts on the **confidentiality, integrity, and availability** of one or more information assets (electronic or non-electronic e.g. paper records) or,

2) a breach of the University's IT Regulations or University Acceptable Use Policy (IT Facilities).

b) **What is required:**
All members of Cardiff University, shall report information security incidents promptly in order that the University can respond in a quick, effective and orderly manner in order to reduce the negative effects of incidents, to repair damage and to inform policy and mitigate future risks.

Managers and Supervisors must:
Ensure that all staff are made aware that the procedure for reporting actual, or suspected, information security incidents is to telephone the **IT Service Desk** on **029 20874487** as soon as possible.

Consideration should be given to:
Training; ensuring that staff and third parties receive adequate and relevant guidance and training, to enable them to identify information security incidents and are encouraged to report them in line with University procedures.

Reporting incidents; 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.

Compliance; failure to report an information security incident to the University may be considered to be a disciplinary matter and addressed under the relevant disciplinary code.

Employees must:
Report information security incidents via the appropriate reporting mechanisms.

Third Parties must:
Report any significant information security weaknesses in the University's systems or services they use or have access to.

c) **What does compliance look like:**
Processes in place to ensure that staff have the necessary training and understanding to recognise information security incidents and take appropriate steps to report incidents.

Staff understand the definition of an information security incident, as described in the Information Security Incident Management Policy and **all** information security incidents are reported to the IT Service Desk.

The University's response to information security incidents is efficient and effective and the process is well understood.

d) **Further information**:
Information Security Incident Management Policy, Information Security Website or Contact us.