

Information Security Framework Review Policy



Version Number:	1.1
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Information Security Framework Steering Group
Effective Date:	19 April 2018
Date of Next Review:	March 2020

1 Purpose

The University's Information Security Framework must remain fit for purpose. Accordingly this policy establishes a requirement for an annual review of the Information Security Framework and defines the objectives and scope of that review and related responsibilities.

2 Scope

This policy covers the University's Information Security Framework using the same scope as set out in the Information Security Policy.

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

4 Policy Statement

The Information Security Framework shall be reviewed annually to determine whether it has achieved its intended outcome(s) over the past year, to review the objectives going forward and to identify opportunities for continual improvement.

5 Policy

5.1 The Information Security Framework shall be reviewed annually to ensure that the Framework as a whole remains fit for purpose and to identify opportunities for continual improvement. The review shall include consideration of the status of actions from previous management reviews; changes in external and internal issues that are relevant to the framework and feedback on the information security performance. The review shall not prevent important and urgent corrective actions being instigated in the interim as a result of information security incidents, as per the Information Security Incident Management Policy.

5.2 The review shall provide:

5.2.1 An assessment of progress towards achievement of the information security objectives as set out in the Information Security Policy, which shall include an assessment of metrics gathered, the outcomes of the key information assets risk assessments and any perceived barriers to implementing the recommended information security controls;

5.2.2 A review of the Information Security Policy with an assessment of the continued relevance of the information security objectives vis a vis the University's strategic objectives and any changes in the external environment;

5.2.3 A review of opportunities for continual improvement including identifying any new metrics to be gathered, modifying the information security controls in place and identifying ways of further embedding information security into the University's normal business processes.

5.3 The outcomes of the Annual Review shall be presented in a report submitted to the Data and Information Management Oversight Group. The report shall be accompanied by an Action Plan with responsibility for each action being assigned to an identifiable individual and a timescale applied. Progress against actions shall be monitored within the year by the Data and Information Management Oversight Group.

6 Responsibilities

It shall be the responsibility of the Senior Information Risk Owner to ensure that an annual review of the Information Security Framework has been conducted in accordance with this policy and action taken as above.