Information Security Framework Testing Policy

Version Number:	2
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Data & Information Management Oversight 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 regular testing of the effectiveness and adequacy of information security controls and defines the objectives and scope of those tests 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 tested regularly to assess the effectiveness and adequacy of the current set of information security controls vis a vis the information security objectives and to identify opportunities for continual improvement.

5 Policy

5.1 The tests shall focus on risk areas identified in the periodic risk assessments of information assets, audit reports, management reviews and information security incident reports as appropriate;

5.2 Tests of the effectiveness and adequacy of current information security controls and related processes may take the form of process reviews, internal or externally delivered vulnerability assessments, network and/or physical penetration tests, using both IT and/or social engineering methods and/or phishing exercises.

5.3 The nature, objectives and timing of any University-wide behavioural testing exercise shall be approved in advance by the Data & Information Management Oversight Group.

5.4 The outcomes of the testing shall be presented in a report submitted to the Data & Information Management Oversight Group and shall inform the annual Information Security Framework Review.

6 Responsibilities

It shall be the responsibility of the Senior Information Risk Owner to ensure that regular testing of information security controls has been conducted in accordance with this policy.