A picture containing text

Description automatically generated

Information Security Framework Testing Policy

# 1. PURPOSE AND SCOPE

## 1.1. 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, defining the objectives and scope of those tests and related responsibilities.

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

# 2. RELATIONSHIP WITH EXISTING POLICIES

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

# 3. POLICY

## 3.1. 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.

## 3.2. 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.

## 3.3. Tests of the adherence to, 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. Tests will use both IT and/or social engineering methods, and/or phishing exercises.

## 3.4. A testing schedule, including the nature, objectives and timing of University-wide behavioural testing exercises, shall be proposed as part of the Annual Review of the framework and be approved by the Assurance and Risk Group.

## 3.5. The outcomes of the testing shall be presented in a report submitted to the Assurance and Risk Group and shall inform the annual Information Security Framework Review.

# 4. ROLES AND RESPONSIBILITIES

## 4.1. The **University Secretary**, in their role as the **Senior Information Risk Owner**, is the sponsor for this policy, and responsible for approving the need to develop or substantively amend the policy, for presenting the final draft to the approving body and for ensuring that their policy-making documents comply with, and are monitored and reviewed in line with the Cardiff University Policy for the Development of Policy-making Documents.

## 4.2. The **Senior Information Risk Owner** is responsible for ensuring that regular testing of information security controls has been conducted in accordance with this policy.

# 5. VERSION CONTROL

|  |  |  |
| --- | --- | --- |
| Document Name | Information Security Framework Testing Policy | |
| UEB Policy Sponsor | University Secretary | |
| Policy Owner | Owen Hadall, Assistant Director IT Service & Operations | |
| Policy Author(s) | Owen Hadall, Assistant Director IT Service & Operations | |
| Version Number | 2.1 | |
| Equality Impact Outcome and Form Submission Date | An EIA has been conducted. The only areas of concern relate to the policy being accessible to those with visual impairments and Welsh speakers. It was noted that specific controls should be assessed as they are created or amended. | 23/01/2023 |
| Privacy Impact Assessment outcome (where applicable) | The risks to privacy and personal data arising from this policy have been assessed and found to be very low as it does require personal data to be collected for its implementation. Proposed tests shall be assessed prior to execution to ensure appropriate handling of any personal data collected. | 23/01/2023 |
| Approval Date | 7th March 2023 | |
| Approved By | Vice-Chancellor (UEB) | |
| Date of Implementation |  | |
| Date of Last Review | 19th April 2018 | |
| Date for Next Review | 7th March 2025 | |
| For Office Use – Keywords for search function | Information, Security, Policy, ISF, Testing, Test | |