

Information Security Metrics Gathering Policy

# 1 PURPOSE AND SCOPE

## 1.1. The purpose of this policy is to establish a framework for the collection of information security metrics which facilitate the management of information security performance at the University.

## 1.2. The scope of this policy includes all currently reportable and potential future metrics which provide insight into information security at the University.

## 1.3. The policy does not include information security metrics at the level of the individual.

# 2. RELATIONSHIP WITH EXISTING POLICIES

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

# 3. POLICY

## 3.1. In order to assess and manage the performance of the University in terms of information security, a comprehensive and relevant set of metrics are required.

## 3.2. Information security metrics should enable one or more of the following:

* Communicate performance.
* Drive improvement.
* Measure the effectiveness of existing controls.
* Help diagnose problems.
* Support decision making.
* Provide increased accountability.
* Guide resource allocation.
* Demonstrate levels of compliance.
* Facilitate benchmarking with peer HEI’s.

## 3.3. The essential features of all metrics to be used in conjunction with this policy are that they should be:

* Necessary to satisfy a specific business requirement.
* Consistently measured.
* Cost effective to produce.
* Quantifiable.
* Expressed using at least one unit of measure (e.g. number of network intrusion events per week).

## 3.4 The category of metrics which will be of most use to the organisation will evolve as the framework matures, risks to information are identified, and in response to changes in external environment. Decisions will need to be made at appropriate junctures as to whether individual metrics are:

* Still useful and to be included in reporting to the Assurance and Risk Group.
* Only useful at an operational level, relevant to the Information Security Oversight Group, and therefore excluded from the Assurance and Risk Group reporting.
* No longer useful and collection to be ceased.

# 4. KEY METRIC TYPES

## 4.1. The metric types used will be a mixture of the below with the trend over time being to move from a predominance of implementation metrics to efficiency and impact metrics.

* Implementation metrics – e.g. % increase over time of encrypted University owned laptops.
* Efficiency/Effectiveness metrics – e.g. % of staff who fall victim to a corporate phishing exercise.
* Impact metrics – e.g. reduction in sensitive data disclosures due to stolen or vulnerable laptops.

# 5. REPORTING

## 5.1. Metrics to be reported will be documented in the Information Security Metrics Matrix that will detail:

* The metric name.
* The purpose of the metric.
* A brief description of the metric.
* What is being measured.
* How it is being measured.
* Who is responsible for measurement.

# 6. ROLES AND RESPONSIBILITIES

## 6.1. 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.

## 6.2. The **Senior Information Risk Owner** is responsible for ensuring that appropriate metrics are collected and analysed as part of the annual review process and used to deliver continual improvement as described in the Information Security Framework Review Policy.

## 6.3. The **Information Security Operations Group** is responsible for maintaining, updating and ensuring the appropriateness of the metrics within the Information Security Metrics Matrix, supplying the Matrix and measurements on request.

# 7. VERSION CONTROL

|  |  |
| --- | --- |
| Document Name | Information Security Metrics Gathering 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 | 1.3 |
| 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. | 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, Metrics |