Information Security Metrics Gathering Policy

Version Number:	1.2
Document Status:	Approved
Date Approved:	19 April 2018
Approved By:	Data and Information Management Oversight Group
Effective Date:	19 April 2018
Date of Next Review:	March 2020

1 Purpose

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.

2 Scope

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

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

3 Relationship with existing policies

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

4 Policy Statement

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.

Information security metrics should:

- 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.

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)

5 Change over time

As the University's maturity of information security management increases, the category of metrics which will be of most use to the organisation will develop. 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 Data and Information Management Oversight Group.
- Only useful at an operational level and to be excluded from the Data and Information Management Oversight group report.
- No longer useful and collection to be ceased.

6 Key Metric Types

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.

7 Reporting

Metrics to be reported will be documented in the Information Security Metrics Matrix which will detail:

- The metric name
- What is measured
- How it is measured
- Who is responsible for measuring

- A brief description of the metric

8 Responsibilities

The Senior Information Risk Owner shall be 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 ISF Review Policy