Information Security Risk Management Policy

Policy Category:	Governance
Subject:	Information Security Risk Management
Approving Authority:	University Executive
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	Business Assurance
Related Procedures:	Information Security Procedure Information Classification Procedure Code of Connection Procedure
Related College Policies:	Enterprise Risk Management Information Security Policy IT Acceptable Use Policy
Effective Date:	9 March 2023
Supersedes:	None
Last Review:	N/A
Next Review:	2024

I. Purpose & Scope

1.1 The purpose of this policy is to ensure that information security risks are anticipated and assessed to effectively manage and treat them proportionately according to a risk tolerance.

1.2 This policy applies to any individual who has access to the university's systems and services and anyone who uses or manages data in any format in the course of university business.

1.3 This policy applies to all information, regardless of the form or format, collectively termed 'Information Assets' which are created or used in support of business activities.

II. Definitions

Data is raw information and statistics collected for reference or analysis, including but not limited to machine readable data, data in print, backups, and archives.

Information is conveyed or represented by a particular arrangement or sequence of things, such as data.

IT System is a place or platform where university data can be entered, stored, or retrieved.

Risk (In accordance with the ISO 27005 definition), is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the university.

Risk Management are the co-ordinated activities, systems and processes in place to direct and control the university with regard to management of risk.

Risk Appetite is the level of risk that the university is willing to tolerate or accept in pursuit of its strategic aims. When considering threats, risk appetite defines the acceptable level of exposure deemed tolerable or justifiable by the institution; when considering opportunities, risk appetite defines how much the university is prepared to actively put at risk in order to realise the potential or expected benefits.

Risk Owner, the person(s) within the Faculty/Directorate/PMO who is accountable for the effective management of risk.

Risk Manager, the person(s) with the Faculty/Directorate who is responsible for the effective management of (a) risk.

Senior Information Risk Owner (SIRO), the person designated by the Principal & President that has overall responsibility for the strategic information security risk management policy. The SIRO will understand how the business goals of an organisation may be impacted by any risks to data, including those related to information security risks.

III. Policy

3. Principles of Information Security Risk Management

3.1 Information security risk management will be assessed through formal and repeatable methods. Assessments will be used to determine risk impact and identify and apply controls appropriate to the risk.

3.2 A documented information security risk assessment process will be used as the basis for identification, definition, and prioritisation of risks.

3.3 Information security risks will be qualitatively labelled as Critical, High, Medium, Low and Minimal and are defined as follows:

a. **Critical Risk** - The risk of imminent compromise or loss of Sensitive Data from either external or internal sources or where Sensitive Data has already been exposed. There is no control in place to protect such Data.
b. **High Risk** - The risk of imminent compromise or loss of Sensitive Data from either external or internal sources. There is only a single control, or multiple ineffective controls, in place to protect such Data.
c. **Medium Risk** - The risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. Controls are in place that are somewhat effective to protect such Data.
d. **Low Risk** - The risk of compromise or loss of Sensitive Data is possible, but not probable or an Information Resource might be used to obtain access to Sensitive Data on a different Information Resource.
e. **Minimal Risk** - There is no realistic risk of compromise or loss of Sensitive Data

3.4 Information Security Risk Treatments will be applied in proportion to the risks identified. The risk will be managed on a continuous basis using one or more of the following methods:

a. Risk elimination, mitigation, or reduction
b. Risk avoidance
c. Risk acceptance
d. Risk transference

3.5 Some risks may be accepted on behalf of the University by person(s) with the appropriate level of authority as determined by the SIRO. Accepted risks will be documented as part of the Information Security KPIs and monitored for links to information security incidents and reported back through the Information Security Strategy Board (ISSB).

3.6 Information risk analysis and treatments will be documented as part of the assessment process and reviewed by Risk Managers

a. The effectiveness of security controls
b. Changes to information resources and operational environments
c. Compliance with regulations, industry standards and University policies

3.7 The frequency of risk monitoring will be based on:

a. Regulatory compliance requirements
b. The sensitivity of the data from the classification label
c. The requirements of the Information Security Policy
d. Risks from interconnectivity of systems

IV. Roles and Responsibilities

4 Strategic leadership, accountability and operational responsibilities are defined below.

4.1 The ISSB has accountability to the University Executive, Council and the Audit, Risk and Compliance Committee for managing information risk. They will direct the information risk appetite for the university and have oversight of the information risk register to escalate risks where necessary via the relevant committees

4.2 The Associate Director of Information Security is responsible to the chair of the ISSB for managing the information risk assessment process and maintaining an up-to-date risk register. Risk assessments may be conducted internally through the Business Assurance Team or external auditors.

4.3 Risk Managers are responsible for agreeing and Risk Owners responsible for implementing appropriate treatments to risks under their control.

4.4 All users must take an active role in identifying and reporting new information risks.

V. Enforcement

5.1 Any action which breaches the terms of the Information Security Risk Management Policy, and its associated policies is an infringement of King's regulations and will be investigated and dealt with in accordance with the appropriate university regulations.

VI. Review and Continual Improvements

6.1 A review of this policy will be undertaken by the Business Assurance Team at a minimum biennially.