INFORMATION RISK MANAGEMENT POLICY

1. Introduction

Information that is collected, stored, analysed, communicated and reported upon is subject to possible misuse, loss, corruption and theft. To counter this the University implements controls to protect information based on an assessment of the risk posed. This assessment balances the likelihood of negative business impact versus the resources that are required to implement the controls (and indeed any unintended negative consequences of the controls).

1.1 Purpose

The purpose of this policy is to state the principles the University will use to identify, assess and manage information risk, whilst aligning itself to the overall University of Reading risk management framework.

1.2 Objectives

The University of Reading's information risk management objectives are that:

- Physical, technical and administrative controls are proportionate and cost effective.
- Physical, technical and administrative controls balance security and user experience.
- Physical, technical and administrative controls are agreed upon by the information asset owner.
- The University identifies, manages and treats information risks based on an agreed risk tolerance.

1.3 Scope

This policy applies to all digital information for which the University has a legal, contractual or ethical responsibility (including that which is stored or processed by third parties on behalf of the University).

Risks shall be categorised by system and actively managed by working alongside information asset owners/stewards/custodians to find and implement effective risk treatment/s.

2. Definitions

Information Asset Owner/Trustee	A senior member of the University who is accountable for its quality, compliance and security.

Data Custodians	Technical expert accountable for efficient data processing systems, including the architecture, correctness and availability of data.
Data Steward	Operational expert accountable for effective data processing, including the collection, creation, modification and deletion of data.

Example:

Information Asset	**Information Asset Owner/Trustee**	**Data Steward**	**Data Custodian**
Staff account details	IT Director	IT Service Desk	Middleware Team
Student data	Head of Student Services	Student Support Services & Operations	SIS
Staff details	HR Director	HR Operations	HR Systems

3. Roles and Responsibilities

Information Asset Owners/Trustees, Data Stewards and Data Custodians	Ensure that information assets are effectively managed in accordance with University policy. Active role in identifying and communicating new risks. Responsible for completing risk assessment forms (and risk acceptance forms) and for agreeing and implementing appropriate risk treatment action/s.
Information Security Team	Shall review submitted risk assessment and risk acceptance forms. Responsible for maintaining the risk register and reporting high rated risks to the DTS Directorate.
DTS Directorate	Alerted to high rated risks and signatory to risk acceptance forms. May work alongside the Information Asset Owner and Information Security Team to review and recommend suitable treatment action.
Information Security Group	Ensure that the University's risk appetite and tolerance is (and remains) appropriate, understood, and communicated and that risk related to the use of IT is identified and managed in-line with policy. Regularly examine and make judgement on the effect of risk on the current and future use of IT at the University.

Senior Information Risk Officer (the University Secretary)	Significant residual risks that remain after mitigation measures are put in place will be referred to the SIRO for consideration and approval/acceptance.

4. Policy

The assessment of information risk is a formal and repeatable method used for identifying risks facing an information asset. It is used to determine impact and identify/apply appropriate controls justified by the risks.

4.1 Risk Assessment

Risks are assessed by considering the likelihood of occurrence and the impact a breach of data confidentiality, integrity and/or availability would have if it did occur.

Risk assessments shall be completed with appropriate/relevant understanding of and access to:

- The legislation to which the University is subject.
- The technical systems in place supporting the University.
- The impact to the University of risks to business assets.
- The University's business processes.

A risk assessment must be completed (at least) for the following:

- Information assets associated with any proposed new or updated systems.
- Information systems associated with information assets classified as restricted or highly restricted.
- Following the discovery of a new risk impacting a system.

4.2 Threats

The University shall consider all high and critical threats that apply to a system whether deliberate or accidental. Threat information shall be obtained from asset owners, users, incident reviewing, contacts across the sector and region, security consultancies, and local and national law enforcement agencies and security services.

4.3 Vulnerabilities

The University shall consider all high and critical vulnerabilities that apply to a system. Vulnerability information shall be obtained from internal sources (e.g. IT personnel, vulnerability scans etc.), technology providers, contacts across the sector and region, security consultancies, and local and national law enforcement agencies and security services.

4.4 Risk Register

The Impact x Likelihood risk score shall form the basis for the risk register. Risks shall be assigned owners alongside a review date and the risk treatment option/s taking place.

The risk register is held in the DTS Operations SharePoint site and access shall be restricted to those with a need to know.

4.5 Risk Treatment

The treatment option will fall into one or more of the following categories:

- *Risk avoidance* (terminate) – There is no cost-effective action to reduce risk. Deciding not to proceed with activities that introduce unacceptable risk to the University.
- *Risk sharing* (transfer) – Shifting part of the risk to other organisations. Common techniques include insurance and outsourcing.
- *Risk modification* (treat) – Information risks are reduced to an acceptable level by introducing, removing or altering controls.
- *Risk retention* (tolerate) – No additional action is required other than what is already in place.

Risk treatment options shall be selected based on the outcome of the risk assessment, and the expected cost/benefit of implementing the options.

The four options for risk treatment are not mutually exclusive. In some cases the University may benefit by using a combination of options such as reducing the likelihood of risks, reducing their consequences, and sharing or retaining any residual risks.

4.6 Residual Risk

Once the risk treatment plan has been defined, residual risk/s need to be determined. This involves an update of the risk assessment, taking into account the expected effects of the proposed risk treatment. If the residual risk still does not fall within the University's acceptable risk criteria, a further iteration of risk treatment may be necessary before proceeding to documented formal sign off via risk acceptance.

4.7 Risk Acceptance

In some cases it may be necessary to accept risk despite it falling outside of normal acceptable risk parameters. This may be necessary because (for example) the benefits accompanying the risks are very attractive, the cost of risk modification is too high, or because appropriate risk treatment cannot be applied within timeframes defined in policy. In such cases, the risk owner (e.g. information asset owner, system owner etc.) must complete a risk acceptance form that explicitly states the risk/s and includes a justification for the decision to override normal acceptable risk criteria.

Risk acceptance forms shall be reviewed and signed off by a member of the DTS Directorate or an appropriate equivalent.

Deviation from any information security/cyber security policy shall require risk acceptance.

5. Related policies, procedures, guidelines or regulations

Key related policies and rules:

- Information Security Policy
- Information Framework
- Information Systems Planning Policy
- Information Classification Policy
- Risk Management Policy
- Business Critical Applications Management policy
- Data Protection Policy.

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
2.0		DTS	Annually	University Policy Group	Nov 19	Nov 19	Nov 20
2.1	Document reviewed. Review frequency changed.	DTS	Biennially	ITD	10/11/2021	11/11/2021	10/11/2023