1 Purpose

This policy outlines the University's approach to information security management and provides the guiding principles and responsibilities to ensure the University's information security objectives are met.

2 Scope

This policy is applicable across the University and individually applies to:

- all individuals who have access to University information and technologies;
- all facilities, technologies and services that are used to process University information;
- information processed, in any format, by the University pursuant to its operational activities;
- internal and external processes used to process University information; and
- external parties that provide information processing services to the University.

3 Objectives

The University's objectives for information security are that:

- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely access information to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve our control environment.

4 Information Security Policy Framework (ISPF)

Information is critical to University operations and failure to protect information increases the risk of financial and reputational losses. The University is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

- all staff complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of the University are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store University information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incident properly investigated and managed;
- Information Asset Owners are identified for all University information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place;

and

- information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, the University will define and implement a set of minimum information security controls, known as the baseline, set out in topic specific information supporting documentation. Where research, regulatory or national requirements exceed this baseline, there is flexibility to increase control at a departmental or project level. The baseline will support the University in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and are available via the information security website.

5 Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **Council** has executive responsibility for information security within the University. Specifically Council is responsible for determining the system of internal controls operated by the University and for monitoring the adequacy and effectiveness of the control environment. The Security Subcommittee of the General Purposes Committee has responsibility for overseeing the management of the security risks to the University's staff and students, its infrastructure and its information.
- **Joint Information Security Advisory Group** (JISAG) has the responsibility to develop and maintain the information security policy framework, review reports on compliance, provide support and guidance, escalate risks and issues, and provide recommendations to the University.
- **Chief Information Security Officer** (CISO) is responsible for establishing and maintaining the University's information security management framework to ensure the availability, integrity and confidentiality of the University's information. The CISO will define and implement the University's information security strategy and lead operational and improvement programmes.
- **Information Security Team** is responsible for maintaining and monitoring compliance against the University's information security policy framework. The Information Security Team will provide services to the University to support a collaborative approach to reducing risks associated with processing University information. The Information Security Team will create and maintain topic specific information security content to support the implementation of information security controls in accordance with the policy framework.
- **Heads of Division** are responsible for the oversight of information security arrangements for departments or faculties within their division in order to ensure that they are functioning in accordance with this policy.
- **Heads of Department and Faculty Board Chairs** are responsible for the effective implementation of this information security policy, and supporting information security rules and standards, within their department or faculty.
- **Users** are required to complete information security awareness training and are responsible for making informed decisions to protect the information that they process.

6 Compliance

The University shall conduct information security compliance and assurance activities to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by the University and may result in enforcement action on a department and/or an individual.

7 Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by JISAG on an annual basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.