Institute of Advanced Research
The University for Innovation

Information Security Policy

1. Introduction

The University is reliant on its information assets to function effectively. It is essential that the University's information assets are protected against the consequences of breaches of confidentiality, failures of integrity and interruptions to availability. An information security breach could damage the University's reputation, cause distress to individuals, and result in litigation.

2. Background

The University has an Information Security Management System which provides a framework for the protection of the University's information assets. This policy forms part of this system. This policy is supported by the other guidance, processes and procedures that form part of the University's Information Security Management System.

3. Objectives

3.1 The primary objectives of this Policy are to: • ensure the protection of all the University's information assets and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets;

• ensure that the University implements good practice;

• ensure that the University's authorised users are aware of and are in a position to comply with all current and relevant legislation;

• ensure that the University's authorised users understand and comply with this policy and the other associated policies and guidance documents;

• ensure that the University's authorised users understand their own responsibilities for protecting, preserving and managing the confidentiality, integrity and availability of the University's information assets; and

• ensure that the University is protected from the potential consequences of security breaches.

3. Scope

This policy applies to anyone with access to the University's information assets including staff, students, visitors and contractors. Information assets include but are not limited to all computers, mobile devices, networking equipment, systems, databases, data files, hard copy documentation, visual media and software.

5. Information Security Principles

5.1 All the University's information assets whether electronic or in hard-copy form must be protected against unauthorised access.

5.2 The University's information assets must be available to all those who have a legitimate need to access them.

5.3 The integrity of the University's information must be maintained so that it is accurate and complete.

5.4 All users of the University's information systems will comply with the University's information security policy and guidance including the IT Use Policy. It is the responsibility of users to ensure that they continually familiarise themselves with and fully understand the contents of the

policies and guidance. Failure to comply with the information security policies and guidance may result in disciplinary action.

5.5 All users of the University's information systems will abide by and adhere to all current legislation as well as regulatory and contractual requirements.

5.6 All the University's information assets will be inventoried.

5.7 All information assets will be classified according to their required levels of confidentiality. The classification of the asset will determine the security controls that will be applied to it and how it must be handled.

5.8 All information assets will be assigned an owner who will be responsible for ensuring that the asset has the correct information classification, has adequate protection and is handled at all times in accordance with its classification.

5.9 Key information assets will be subject to annual risk assessments to identify the probability and impact of security failures. The results of the risk assessments will determine the appropriate security controls to be applied to the assets.

5.10 All users of University's information systems shall receive information security training appropriate to their role and to the classification of information assets they have access to.

5.11 All suspected and actual information security breaches must be recorded and reported to the IT Administrator, who will then refer any significant breaches to the Registrar if required.

6. Information Security Responsibilities

6.1 The University Management Committee

The University Management Committee has the ultimate responsibility for information security at the University. The University Management Committee will ensure that the University complies with relevant external

requirements including legislation and contractual obligations. The University Management Committee is responsible for the overall direction and commitment to information security. The Committee will approve information security policies and guidance, provide high level support for security initiatives and review the adequacy of the University's Information Security Management System. Deans and HoDs will take responsibility for operational compliance within their areas of responsibility.

6.2 Information Risk Owners

HoDs and Deans will be the Information Risk owners, who will be responsible for being the focal point within their departments for the escalation and resolution of identified information security risks. They will be responsible for making risk based decisions on requests or changes that are outside of normal working practices or that are exceptions to policy.

6.3 Information Security Manager

The Registrar will be the Information Security Manager, who will be responsible for:

• creating, reviewing and maintaining information security policies and guidance;

• monitoring and reporting on information security within the University;

• undertaking risk assessments of key information assets;

• evaluating security technologies, processes and the implementation of appropriate levels of security control;

• assessing the adequacy of information security controls for new or changed systems/services;

• providing an advise on information security; and

• investigating suspected or actual security incidents.

6.4 Information Security Steering Committee

University Management Committee will be the Information Security Steering Committee which considers all matters concerning the management of information security and information governance. The committee:

• considers information security, Right to Information policies and guidance documents prior to submission to the University Board;

• evaluates and reports on the potential impact of proposed information governance and security controls on all areas of the University;

• reviews and monitors information security incidents and the implementation of any actions which arise;

• identifies and reports on new potential information security risks;

• reviews the implementation and effectiveness of the Information Security Management System components and information governance requirements;

• identifies and oversees training requirements to increase staff awareness of the information security and Right to Information legislation and other information security matters;

• reviews information security and information governance audit findings and recommendations and monitors the implementation of those recommendations;

• promotes the effective management of all University information, in all formats, to meet both the needs of the University and legislative requirements; and

• promotes a University-wide culture which promotes personal accountability for the appropriate management of information.

6.5 HoDs and Managers are responsible for ensuring that their members of staff:

• have the correct level of access to data assets;

• have read and understood the University's information security policy and guidance;

• comply with the University's information security policy and guidance; and

• have undertaken the appropriate information security training.

HoDs and Managers will investigate in a timely manner any security concerns that their staff may have and if necessary report them to the Information Security Manager.

6.6 All Staff, Students and Third Party Visitors and Contractors

All the University's system users are responsible for complying with the University's information security policies and guidance. All University system users will sign the IT conditions of use before being supplied with their network account credentials. Users are responsible for reporting any suspected security incidents immediately to the IT Administrator or if appropriate to their HoD or Manager.