UCA Information Security Policy

Version 2.3

Approved by: Board of Governors
Date approved: 30/11/2021
Review period: Annual
Date reviewed: 04/11/2021
Owner: Director of IT Services

Table of Contents

1.0 Document Change Control

Version	Status / purpose of change	Author	Date
Draft		Janine Travers / Marion Wilks	25/08/2020
2.2	Update and reformat from previous policy	Janine Travers	26/08/2020
2.3	Gramatical and small terminology updates throughout, with a change to the roles and responsibilities to align to the Director or IT Services and the University DPO.	Janine Travers	15/09/2021

2.0 Overview

This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect the University's information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

The aim of this policy is to ensure that staff and students of UCA all understand the importance of Information Security Management as it relates to the information they gather, process and store and the legal and ethical responsibilities that are incumbent on them both as individuals and as members of UCA.

Compliance with this policy is necessary to ensure the protection of the University's reputation and success within academic, administrative and information sharing activities and to ensure business continuity, and minimise damage by preventing and minimising the impact of security incidents.

This policy will be reviewed and published annually. It will be made available via the University website to all staff, students and anyone working for or on behalf of UCA and annual communications will be distributed to confirm the updated release.

3.0 Objectives

The objective of this Information Security policy is to ensure that all information and information systems upon which the University depends are adequately protected to an appropriate level; ensure business continuity and minimise damage by preventing and minimising the impact of security events and incidents. In particular, information assets must be protected in order to ensure:

- Confidentiality: the prevention of the availability and disclosure of information to unauthorised individuals, entities or processes.
- Integrity: the safeguarding of the accuracy and completeness of (information) assets.
- Availability: The accessibility and usability of information upon demand by an authorised entity.

Ensure compliance with all current and relevant legislation, and ensure users are aware of the expectation and responsibilities in relation to these laws and the associated University policies and procedures.

Review and enforce this policy and associated documentation.

Ensure that this policy protects the University from liability or damage through the misuse of its information systems facilities.

Ensure that adequate training in relation to this policy is made available and regularly updated and monitored.

4.0 Scope

This policy applies to:

All members of the University (staff, students, external members of statutory committees); visitors to the University; partners with and sub-contractors to the University; and any other authorised users of the University's information.

All information processed by UCA in pursuit of all its operational and academic activities, regardless of whether it is processed electronically or in paper form.

The lifecycle of the information from creation through storage, transmission, utilisation to disposal.

All information transferred or exchanged with third parties, or held by third parties on behalf of UCA, regardless of whether it is processed electronically or in paper form.

5.0 Roles and Responsibilities

The Director of IT Services in consultation with the Universiy Data Protection Officer shall be responsible for ensuring that the University's information security objectives are aligned with the organisation's objectives.

The UCA Director of IT Services in consultation with the Universiy Data Protection Officer shall be responsible for ensuring that appropriate security, legal and regulatory controls are identified, implemented and maintained by information owners. They shall be supported in this task by all staff.

The Director of IT Services in consultation with the Universiy Data Protection Officer shall be responsible for ensuring that appropriate and effective information security controls are monitored and reviewed to ensure compliance with the UCA's legal regulatory or contractual obligations.

Information asset owners within UCA shall be responsible for the identification, implementation and maintenance of controls for the information assets they own whether in electronic or hardcopy and the risks to which they are exposed.

The Director of IT Services and Head of Networks, Security and Compliance are responsible for setting the priorities for the information security work programme. A programme of reviews and assessments of security effectiveness will form part of this programme, and will establish an agenda for security improvements.

Heads of School, Directors and Heads of Departments are responsible for ensuring that information and information systems used within their Schools/departments are managed and used in accordance with information security policies, protocols and guidelines.

All staff whether permanent or temporary are responsible for the protection of the UCA's information assets, enabling the confidentiality, integrity and availability of these assets to be maintained.

All third party suppliers to the UCA must be informed of this policy through the tendering process and are required to conform to it.

All staff and students must adhere to all policies relating to Information Security. Non-compliance will be subject to investigation and may result in disciplinary action under UCA's disciplinary procedure.

6.0 Policy Statement

a. This information security management policy outlines the University's approach to information security management. It provides the framework for describing the guiding principles and responsibilities necessary to safeguard the security of the University's information systems. These principles responsibilities are set out in this policy and supporting policies, codes of practice, procedures and guidelines.

b. The University is committed to developing and implementing a solid framework of Information Security Management. It aims to ensure the confidentiality, integrity and availability of its information by adherence to the principles defined in this policy, and will be applied to all of the physical and electronic information assets for which the University is responsible.

c. The University will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security.

d. In particular, business continuity and contingency plans, data backup procedures, avoidance of malicious code and compromise, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are supported by specific documented policies, procedures and guidelines.

e. These commitments are made in the recognition that adherence to these principles is consistent with the mission and values of the University and critical to its core business; strategic plans; and legal, regulatory and contractual requirements.

f. These commitments will be embedded within the University's strategic and business planning and its risk management, major incident recovery and business continuity arrangements.

7.0 Risk Management

A systematic approach to information security risk management has been adopted by UCA to identify business needs regarding information security requirements (including legal, contractual and regulatory) and to create an effective operational information security framework.

Information security risk management is not a one-off exercise with a single set of control recommendations which remain static in time but a continual process.

The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk management and risk acceptance and independent of technology or software

8.0 Legislation and Standards

The list below contains some of the legislative and regulatory requirements UCA must comply with:

Data Protection Act 2018
The General Data Protection Regulation
Freedom of Information Act 2000
Human Rights Act 1998
Computer Misuse Act 1990
Companies Act 2006
Health & Safety at Work Act
Employment Legislation
Bribery Act 2010
Fraud Act 2006
Regulation of Investigatory Powers Act 2000
The Payment Card Industry Data Security Standard

9.0 Compliance

All members of the University have a responsibility to ensure that they are aware of and comply with this policy and all supporting University policies, procedures and guidelines. Each individual is responsible for protecting the University's information assets, systems and IT infrastructure.

Failure to comply with this policy could result in potential disciplinary action.

10.0 Related Policies, Standards and Procedures

- IT Use Policy
- Data Protection Policy
- ITS Email Usage Policy