Information Security Management Policy

INTRODUCTION

Administrative data and systems are resources and assets owned by and entrusted to the University. This document sets out the University's commitment and policy in relation to the management of the security of these resources.

SECURITY PRINCIPLES

UCD generates, manages and is entrusted with private, confidential and sensitive information. The University is committed to protecting the confidentiality of all our information and ensuring that information is accurate, complete & available for appropriate uses. To achieve this, we set out the following security principles.

a) **Appropriate Access**- Access to administrative data and systems shall be provided to those authorised as necessary to facilitate the conduct of University activities.

b) **Protection of integrity**- Information resources shall be managed to ensure that they remain accurate, trustworthy and reliable by ensuring they are protected from theft, misuse, corruption and loss.

c) **Risk based protection**- Data and systems shall be protected in a manner appropriate to the risks to the resources and the University's needs.

d) **Compliance**- Information resources shall be managed to ensure compliance with external regulation, governance and statutory requirements.

e) **Continuous review** –Protection mechanisms and processes shall be reviewed to ensure that they are effective, relevant and appropriate to meet the needs of the University.

ORGANISATION OF INFORMATION SECURITY MANAGEMENT

UCD's administrative systems and data are managed, used and developed by several elements of the organisation. This policy sets out specific roles associated with the management of information security at UCD.

A security management framework and policies for the management of Information Security is defined where:

IT Services, under the authority of the CIO, is the ***System Manager*** for Information resources. IT Services implement specific procedures which enforce access authority and establish guidelines and standards for Systems and Data security under this Policy.

Nominated ***Information Owners*** have the authority to grant or revoke access to Data or Systems which use Data, and define the classification and controls over the use of data.

The CIO shall define the minimum standards and procedures for system security for all systems managing information under the UCD Information Security Policy.

IT Services shall also establish procedures for the communication of policies, guidelines and procedures created under the security framework.

Controls and provisions must be agreed between relevant authorities including the Information Owner, System Manager and the Information Security Officer subject to the policies indicated by the Information Classification policy.

End user policy and guideline documentation is to be made available to all users. These policies must be appropriate to the proper use of the systems and the classification of the data held on the system, and may be based on appropriate technical standards.

SYSTEM MANAGER REQUIREMENTS

System Managers are required to ensure that information systems are managed in accordance with the security needs of the information resources they control or access.

Security needs are identified through the processes and procedures defined in the Security Assurance and Information Classification Policies, and related procedures.

System Managers shall define and implement standards and procedures to ensure that systems are managed in a manner appropriate to their security needs.

System Managers must provide assurance to Information Owners that security is adequately managed & maintained, by providing evidence of documented procedures, metrics, or security testing in a manner consistent with the requirements of the Security Assurance Policy.

Records of System Managers and systems shall be maintained by the Information Security Officer.

INFORMATION OWNER REQUIREMENTS

For each administrative office, application or system, an appropriate group of Information Owners must be nominated by the Administrative Systems IT Steering Group. The Information Owner is then responsible for compliance with this policy.

A schedule of all Administrative Information Owners and assets shall be maintained by the Information Security Officer.

Information Owners must confirm that periodic assessments are performed on systems which access and manage their information. For new systems, or significant changes

to system functionality, this assessment is carried out as per the security assurance policy.

Where security risks are deemed to be significant, Information Owners must confirm that appropriate controls are implemented, and reviews or assessments are performed periodically.

Where non-UCD staff or third parties are granted access to sensitive data, Information Owners must ensure that regulatory & legal requirements- such as Data Protection- are met by the 3rd party. This may require that UCD perform a security assessment, or that the 3rd party provides UCD with certification or an independent review.

End user access is granted to systems under the authority of the Information Owner for that application. Control of systems management access and system level privileges is managed by the System Manager.

Information owners exercise their responsibilities in this area using the supporting roles of the Security Working Group and the Information Security Officer.

INFORMATION SECURITY OFFICER RESPONSIBILITIES

An Information Security Officer shall be nominated by the CIO to perform the following roles:

Implementation of effective and practical technologies and processes to secure the network and computing infrastructure of the University.

Development and implementation of a security awareness programme to meet the needs of Information Owners, System Managers, and all other users of information resources of the University.

Development and implementation of systems assurance and incident procedures to assess the risks and incidents associated with the introduction, modification and operation of Information Systems of the University.

Recommending effective and practical policies and practices related to information assurance and security to the Security Working Group, Information Owners, System Owners, and the CIO.

SECURITY WORKING GROUP RESPONSIBILITIES

A Security Working group shall be established to recommend Security Policy, standards and guidelines to the Administrative Systems IT Steering Group. This group shall be concerned with the following activities:

a) Ensuring security policies continue to meet the needs of the University; are adequate to meet regulatory requirements, and are in line with best practice.

b) Ensuring security policies in place are appropriately implemented.

c) Review of security risks that are relevant to UCD, including review of security assessments and incidents, to be reported by the Information Security Officer.

This group shall meet regularly as required, no less than twice per annum. Meetings are scheduled at the request of the CIO. Representative Information Owners and System Managers shall form the membership of the Security Working Group, together with the Information Security Officer and other members nominated by the CIO.

A security assurance process shall be defined to assess the risks and incidents associated with the introduction, modification and operation of Information Systems. The findings of assessments shall be reported to the Security Working Group by the Information Security Officer. System Managers and Information Owners are required to ensure that projects which impact information or systems registered under Security Policy are assessed under this process.

END USER POLICY

It is the responsibility of ***all Staff*** to protect the University's data from unauthorised change, destruction or disclosure.

SCOPE OF POLICY

This policy applies to all electronic administrative systems and data.