Information Security Policy

Section 1 - Background Information

(1) Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities. This document sets out the Australian Catholic University (ACU) Information Security Policy for use by all members of the ACU community.

(2) The Policy is directly aligned with the Information Security Industry standard AS/NZS ISO/IEC 27002:2013(E) Information technology - Security techniques - Code of practice for information security management. Relevant sections from this standard are directly referenced in this document.

Section 2 - Policy Purpose

(3) Data, information and the underlying technology systems are essential assets to ACU and provide vital resources to staff and students and consequently need to be suitably protected.

(4) Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that specific security and University objectives are met.

(5) The University is committed to providing a secure, yet open information environment that protects the integrity and confidentiality of information without compromising access and availability.

(6) The purpose of this Policy is to:

a. set out the security requirements that ACU must meet in order to manage the Confidentiality, Integrity, Availability and Privacy of University owned data and information; and
b. ensure the University can meet its obligations with applicable laws, regulations, and standards.

Section 3 - Policy Documentation

(7) This Policy is expressed by documents that are split into two sections: this Policy, and the accompanying Information Security Procedure for compliance with the Policy. Each section is subject to review and change as needed. Additional sections may be added.

Section 4 - Application of Policy

(8) This Policy applies to all information that is electronically generated, received, stored, printed, filmed, or keyed; and to the IT applications and systems that create, use, manage and store information and data. The Policy covers the following areas:

a. Access Control
    i. Objective: To limit access to information and information processing facilities in support of business requirements.

b. Digital Messaging
    i. Objective: To establish and maintain the protocol for using Digital Messaging in all its forms, including the security aspects of information transfer within the University and with any external entities.

c. Communications and Operation Management
    i. Objective: To ensure the protection of information and the secure operations of networks and supporting processing facilities.

d. Physical and Environmental Security
    i. Objective: To prevent unauthorised physical access, damage and interference to the University's information and information processing facilities.

e. System Acquisition, Development and Maintenance
    i. Objective: To ensure that information security is an integral part of information systems across the entire life cycle. This includes information systems that provide services over public networks.

f. Supplier Relationships
    i. Objective: To ensure protection of the University's information assets that are accessible by Service Providers.

g. Information Security Incident Management
    i. Objective: To ensure a consistent and effective approach to the management of information security incidents, including security events and vulnerabilities.

h. Information Security aspects of Business Continuity Management
    i. Objective: To ensure information security continuity is embedded in business continuity plans and management processes.

i. Compliance Management
    i. Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

Formal processes and procedures covering these key areas are set out in the Information Security Procedure.

(9) The provisions of this Policy apply to all ACU, students and staff, (including temporary agents and staff engaged under contract). This Policy includes, but is not limited to:

a. university information in any form, including print, electronic, audio, video, and backup and archived data. This includes, computer systems, peripheral devices, software applications, databases, middleware and operating systems;
b. physical premises occupied by the personnel and equipment;
c. operational environments including power supply and related equipment;
d. processes and procedures; and
e. transmission of Communications and related pathways.

Section 5 - Policy Principles

(10) This Policy defines the principles for establishing effective security measures to ensure the Confidentiality, Integrity, Availability and Privacy of University information. The Policy also covers the continued availability of information and the Information Environment to support University business activities, including the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification,

removal or copying.

(11) The following principles outline the minimum standards that guide the University's Information Security processes and procedures and must be adhered to by all members of the ACU community.

University Responsibilities

(12) The University is responsible for safeguarding the ACU Information Environment and Information Resources against security threats. The University discharges its responsibilities through the following and the set of measures outlined in the Information Security Procedure:

a. defining roles and responsibilities and establishing clear lines of accountability;
b. protecting the University's information assets against internal and external threats (e.g. security breach, loss of data);
c. ensuring that the University complies with applicable laws, regulations, and standards;
d. identifying and treating security risks to the University's information environment through appropriate physical, technical and administrative channels; and
e. developing best practices for effective Information Security across the University.

User Responsibilities

(13) Users must abide by all relevant laws and all University policies.

(14) Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment.

(15) Users may only access information needed to perform their authorised duties.

(16) Users are expected to determine and understand the classification of the information to which access has been granted through training, other resources or by consultation with the relevant supervisor or the Data Steward.

(17) Users must protect the confidentiality, integrity and availability of the University's information as appropriate for the information classification level.

(18) Users may not in any way divulge, copy, release, sell, loan, alter or destroy any information, except as authorised by the relevant University delegate.

(19) Users must safeguard any physical key, ID card or computer / network account that enables access to University information. This includes maintaining appropriate password creation and protection measures as set out in the password composition guidelines.

(20) Any activities considered likely to compromise sensitive information must be reported to the relevant supervisor or to the IT Security Officer.

(21) Users are obliged to protect sensitive information even after separation from the University.

Managers and Supervisors

(22) In addition to complying with the requirements listed above for all staff and contractors, managers and supervisors must:

a. ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Data Stewards, and that those procedures are followed;

b. ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic; and
c. ensure that each staff member understands their information security related responsibilities.

System and Technology Managers

(23) In addition to complying with the stated Policy requirements defined for all staff, contractors, managers and supervisors, system and information environment managers are responsible for:

a. ensuring adequate security for computing and network environments that capture, store, process and / or transmit University information;
b. ensuring that the requirements for confidentiality, integrity and availability as defined by the appropriate Data Steward are being appropriately managed within their respective environments;
c. understanding the classification level of the information that will be captured by, stored within, processed by, and / or transmitted through their technologies; and
d. developing, implementing, operating and maintaining a secure information environment that includes:
    i. a cohesive architecture;
    ii. system implementation and configuration standards;
    iii. procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Data Stewards; and
    iv. an effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "information management best practices" for the system or service.

Section 6 - Risk Assessment and Treatment

(24) Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational damage likely to result from security failures.

(25) The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

(26) Responsibilities for Risk Assessment and Treatment are clearly defined in the Risk Management Policy and Risk Management Procedure.

Section 7 - Information Classification

(27) ACU information is classified under four broad classification headings:

a. Internal Restricted
b. Internal Protected
c. Internal General
d. Public Access

(28) The ICT Governance Policy sets out the access rights, roles and responsibilities of ACU staff in relation to the management and protection of information. Further detail about the classification of information is listed in Section 10.

Section 8 - Roles and Responsibilities (associated with this Policy)

Approval Authority

(29) The Vice-Chancellor and President is the Approval Authority for this Policy.

Governing Authority

(30) The Information Communication and Technology Advisory Committee (ICTAC) is the Governing Authority for this Policy and the Chief Operating Officer is the Chair of the Committee.

Responsible Officer

(31) The Chief Information and Digital Officer is the Responsible Officer for this Policy.

(32) Specific responsibilities associated with this Policy include monitoring compliance with this Policy.

Section 9 - Policy Review

(33) Unless otherwise indicated, this Policy will still apply beyond the review date.

Section 10 - Definitions

(34) To establish operational definitions and facilitate ease of reference, the following terms are defined as they relate specifically to this Policy.

Term	Definition
Access Control	is the selective restriction of access to the ACU information environment and/or ACU information resources.
Authorisation	is the function of specifying access rights to information resources.
Availability	refers to ensuring that information assets are available for their intended use.
Confidentiality	of information assets refers to limiting information access and disclosure to authorized users, and preventing access by or disclosure to unauthorized ones.
Data or Institutional Data	is a general term used to refer to the University's information resources and administrative records which can generally be assigned to one of four categories: 1. Public access data – data that is openly available to all staff, students, and the general public. 2. Internal general data – data used for University administration activities and not for external distribution unless otherwise authorised. 3. Internal protected data – data that is only available to staff with the authorized access in order to perform their assigned duties. 4. Internal restricted data – data that is of a sensitive or confidential nature and is restricted from general distribution. Special authorisation must be approved before access or limited access is granted.

Term	Definition
Data Steward	is a Member of the Executive who oversees the capture, maintenance and dissemination of data for a particular Organisational Unit. Data Stewards are responsible for assuring the requirements of the Data and Information Governance Policy and the Data and Information Governance Procedure are followed within their Organisational Unit. Data Stewards also have delegated responsibility for information assets, including defined responsibilities for determining appropriate classifications of information, defining access rights and ensuring that information asset risks are identified and managed. One or more Data Managers may be defined for an information asset, with some responsibility for operation of the asset delegated by the data steward.
Information Asset	is any set of information or part of the Information Infrastructure critical to the functioning of the University. Every information asset has a delegated system owner.
Information Environment	includes the buildings, permanent installations, information services, fixtures, cabling, and capital equipment that comprise the underlying system within or by which the University: 1. generates, stores, transmits, manages, uses, analyses, or accesses information; or 2. transmits communication.
Information Resources	is a general term used to refer to the University's information resources and administrative records, the term in intended to include information and data (structured or unstructured) stored in print, digitally, or in any other format. 1. Structured Information usually refers to data captured and stored in University Enterprise systems, databases and spreadsheets. 2. Unstructured Information as it refers to this Policy - is all information that cannot be easily classified to fit within the structured area. Photographs, graphic images, video, webpages, pdf files, PowerPoint presentations, emails, blog entries, wikis and word processing documents fall within the unstructured area.
Information Security	is the set of measures by which the University seeks to treat risks to the confidentiality, integrity and availability of its information assets.
Information Security Risk	measures the potential loss of an asset's confidentiality, integrity, or availability. Risks are defined by a combination of threats, vulnerabilities and impacts — a threat exploiting vulnerability results in an impact. Risks can be accepted (if the cost of treating the risk outweighs the cost of the impact), mitigated (through applying appropriate controls) or transferred (through insurance).
Integrity or Data Integrity	refers to the accuracy and consistency of data over its entire life-cycle.
Member of the Executive	is defined as the positions, which normally report to either the Vice-Chancellor and President or a Member of the Senior Executive, and in an area of responsibility published on the University's Organisational chart.
Password	is a word, or string of characters used for user authentication to prove identity to gain access to a resource.
Passphrase	is a sequence of words or other text used to control access to a computer system, program or data where this functionality is available. A passphrase is similar to a password in usage, but is generally longer for added security.
Privacy	The University will comply with all current Privacy related legislation in particular, the Privacy Amendment (Private Sector) Act 2000 (Cth) (the Privacy Act).
Quality or Data Quality	Refers to the validity, relevancy and currency of data.
Security	Refers to the safety of University data in relation to the following criteria: 1. access control; 2. authentication; 3. effective incident detection, reporting and solution; 4. physical and virtual security; and 5. change management and version control.
Standards (mandatory) and guidelines (recommended practices)	will be published as attachments to this policy to assist users, system owners and data stewards to meet their IT security responsibilities. These standards and guidelines, though presented as attachments, are an integral part of this university's Information Security Policy.
Threat	is any technological, natural, or man-made cause of harm to an information asset.

Term	Definition
Vice-Chancellor's Advisory Committee (VCAC) (also Member of the Senior Executive)	is the peak senior strategic forum of ACU. The Vice-Chancellor and President chairs VCAC, membership of the group inclused the Provost and Deputy Vice-Chancellor (Academic); Chief Operating Officer; Deputy Vice-Chancellor (Research and Enterprise); and Deputy Vice-Chancellor (Education).
Vulnerability	is a weakness in the security of an information asset that might be exploited by a threat, such as a software bug, unlocked room or well-known or readily identifiable password.

Status and Details

Status	Current
Effective Date	28th February 2024
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	28th February 2024
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Russell Parker Chief Information and Digital Officer
Enquiries Contact	Information Technology