Information Security Policy

Purpose

The purpose of this document is to provide direction on information security and how WentWest seeks to protect the confidentiality, integrity and availability of the information of WentWest and its stakeholders, with whom information is either shared or held by WentWest, in accordance with the requirements of the ISO 27001:2022 standard on information security management systems.

Introductory comments

WentWest is committed to implementing an information security management system that satisfies the requirements of information security and to the continuous improvement of the system, in accordance with the WentWest Management System Framework.

WentWest recognises the importance of information as an asset that enables the effective functioning of the business and enables fulfillment of its mission. Information security management is a mechanism to ensure business continuity and to minimise organisational harm by preventing or minimising security incidents and their impact through a risk-based approach. It enables sharing of information to authorised recipients, while also ensuring its protection from unauthorised changes or deletions.

This policy is to be reviewed in line with changes occurring to the WentWest Management System; and to be communicated to all staff when updated.

Scope

This policy applies to all WentWest employees as well as external stakeholders with whom information is shared, through contractual agreements.

Associated Documents – Refer Document Repository

WentWest Management System Framework
WentWest Information Security Manual

Standards & Legislation

Privacy Act 1988 (Cth)
ISO 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems - Requirements
ISO 27002:2022 - Information security, cybersecurity and privacy protection – Information security controls
Health Records and Information Privacy Act 2002 (NSW)

Acronyms & Definitions

Availability	Characteristic of the information by which it can be accessed by authorised persons when it is needed.
Confidentiality	Characteristic of the information by which it is available only to authorised persons or systems.
Earned autonomy	Reduced reporting requirements and scrutiny earned through consistently positive performance outcomes.

Employee	In relation to this policy, an employee refers to an individual who is employed by WentWest and has authorised access to WentWest's computer systems, networks, and data. Workers typically include employees, contractors, subcontractors, secondments, agency staff, student placements, work experience students and other individuals who have a formal working relationship with WentWest.
Information	WentWest creates, collects, processes, stores, transmits and disposes of information, which includes data, in many forms, such as electronic, physical and verbal (e.g. conversations and presentations). The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information.
Integrity	Characteristic of the information by which it is changed only by authorised persons or systems in an allowed way to ensure the accuracy, completeness and consistency of data over its entire life cycle.
Information Security	Preservation of availability, confidentiality and integrity of information assets, including digital, physical, or intellectual.

Policy

Information Security Objectives

Enterprise objectives

WentWest is committed to achieving the following enterprise Information Security objectives:

1. attain and maintain an information security management system compliant with ISO 27001 standard in order to:
    a. strengthen applications and increasing scope of eligibility for grant and research funding opportunities
    b. establish WentWest as a trusted partner for data custodianship
    c. improve the confidence level of our stakeholders
    d. minimise rigorous checks and seek 'earned autonomy' with key external stakeholders
    e. minimise information security events, incidents and breaches
2. ensure the privacy of personally identifiable information handled by WentWest:
    a. through rigorous policies and procedures
    b. by ensuring the correct use of labelling, secure storage and appropriate access controls
3. ensure the effectiveness of information security controls through monitoring and review of all function specific objectives relevant to information security
4. ensure that the information security components of the WentWest Management System (WMS) are suitably resourced

These objectives are tracked in Directorate and/or team plans.

Function objectives

To support enterprise information security objectives, function-specific objectives must be identified within directorate and/or team plans and the approach to achieve the following outcomes:

- Availability of information assets to authorised users when needed
- Flexible and responsive mechanisms that accommodate changes in individual responsibilities and organisational structure

- Fit-for-purpose protection for the organisation's information assets, while minimising inconvenience to authorised users
- Ensuring appropriate access controls are established
- Monitoring access to information assets to inform appropriate actions
- Limit the use of information assets to the business purposes for which they are intended
- Preservation of information integrity by preventing information from being subject to unauthorised modifications and corruption
- Streamlined policies and processes around information security management
- Ensure information retained by WentWest is relevant and appropriate to be held in line with regulatory requirements and reasonable expectations of interested parties
- Ensure information security objectives and their proposed outcomes are communicated across WentWest

Information Security Principles

PRINCIPLE 1: Information is a WentWest Asset
WentWest recognises information as a valuable asset which should be protected.

PRINCIPLE 2: Controlled Access to Information
All forms of access to WentWest information shall be controlled.

PRINCIPLE 3: Controlled Access to Networks & Computer Systems
All connections to WentWest networks & computer systems shall be authorised and controlled.

PRINCIPLE 4: Login Mechanism as Authorisation
All users of WentWest computer systems are to be authorised by the use of a verification process.

PRINCIPLE 5: Individual Accountability
Individuals shall be held accountable for their use of WentWest information assets and for activity performed under their personal login identities.

PRINCIPLE 6: Definition of Functional Responsibilities
Definitions of the functional responsibilities of owners, stewards, custodians, and users of data shall be clearly stated and form the basis of delegating the accountability for information security.

PRINCIPLE 7: Use of Unauthorised Software
Use of unauthorised or illegal software is prohibited.

PRINCIPLE 8: Contingency Plans
Plans for disaster recovery and business continuity shall be prepared, documented, and regularly tested for all information systems which are essential to WentWest's internal operations.

PRINCIPLE 9: Information Assets held by third parties, including the Cloud
All WentWest information assets that are held by third parties, including cloud services are subject to WentWest Information Security Policies and providers of these services shall comply with contractual requirements.

PRINCIPLE 10: External Distribution of Information
WentWest Information assets shall only be distributed to external parties, in accordance with our labelling and classification principles

PRINCIPLE 11: Access to Patient Information While Overseas
Patient information shall not be accessed while travelling overseas to ensure compliance with the Health Records and Information Privacy Act.

PRINCIPLE 12: Commitment to Continuous Improvement
WentWest is committed to continuous improvement of the information security components of the WentWest Management System.

PRINCIPLE 13: Commitment to Satisfy Information Security Requirements
WentWest is committed to ensuring that all information security requirements are satisfied in accordance with the identified risk.

Exemptions

In the event of exceptional circumstances, an exemption may be granted from this Information Security Policy. Specific written approval shall be obtained from a senior executive manager, dependent upon the nature of the policy being exempted. The exemption must meet the following criteria:

- A legitimate business reason exists;
- No other solutions which conform to this policy exist;
- An information security risk assessment has been completed;
- Risk owners have been identified who accept accountability for the risks

Education and Compliance

WentWest is to ensure that employees are provided training and awareness opportunities relating to the requirements of this policy and their individual responsibilities for information security. This will be covered in employee induction and will continue through meetings, staff updates and ongoing training sessions.

Any breaches of this Information Security Policy, whether inadvertent or deliberate, jeopardise the security of WentWest's information assets and may be subject to disciplinary action in alignment with employee contracts and Performance Counselling and Disciplinary Policy.

This policy is approved and issued by the CEO of WentWest Limited.

CEO: DocuSigned by: Roy Messom 8ED15789553E482... Date: 11-Sep-2023