

Information Security Policy

January 2026

TEMPLATE ONLY





[THIS PAGE IS INTENTIONALLY LEFT BLANK]





Contents

Data Retention and Deletion Policy	1
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
5. Data Protection and Privacy	5
6. Roles and Responsibilities.....	5
7. Policy Compliance	6
8. Related Standards, Policies and Processes	6
9. Revision History	6





1. Introduction

[Company Name] relies on information for its operations, decision-making, service delivery, and compliance obligations. Protecting information from unauthorised access, disclosure, modification, or destruction is essential to maintain trust, support business objectives, and reduce risk.

2. Purpose

This policy defines how [Company Name] manages technology, from hardware and software to networks and access. Its goal is to:

- Keep our systems secure and reliable.
- Ensure everyone uses IT resources responsibly.
- Protect sensitive and personal data.
- Support compliance with legal, regulatory, and contractual obligations.

3. Scope

This policy applies to:

- All information and data processed, stored, or transmitted by the organisation
- All systems, applications, endpoints, servers, and backup environments
- All employees, contractors, and third-party users
- All Data formats, including electronic and physical records.

4. Policy

[Company Name] will implement measures to ensure information is protected from threats that may compromise confidentiality, integrity, or availability. All staff, contractors, and third parties must comply with the following principles:

4.1 Access Control

- Access to information must be based on business need and role responsibilities
- Multi-factor authentication must be implemented where technically feasible
- User access must be reviewed regularly

4.2 Data Protection

- Sensitive and confidential information must be protected both in transit and at rest
- Personal information must be handled in accordance with privacy legislation and internal privacy policies
- Anonymisation or de-identification must be applied where practical





4.3 System Security

- Systems and applications must be patched and updated to minimise vulnerabilities
- Security logging and monitoring must be implemented to detect and respond to incidents
- Backups must be performed regularly and securely stored to support recovery

4.4 Physical Security

- Physical access to offices, servers, and storage media must be controlled
- Paper and media records must be securely stored and destroyed when no longer required

4.5 Incident Management

- Suspected or actual security incidents must be reported immediately
- Incidents must be investigated, contained, and documented
- Lessons learned must be incorporated into security practices

4.6 Information Lifecycle Management

- Information must be retained only as long as necessary for business, legal, or regulatory purposes
- Secure deletion or destruction must occur once retention periods expire or information is no longer required
- Legal or regulatory holds take precedence over routine deletion

4.7 Third-Party Security

- Contractors, vendors, and partners must comply with [Company Name] security requirements when handling organisational information

5. Data Protection and Privacy

All handling of sensitive, confidential, or personal data must comply with relevant legislation, including the Privacy Act, GDPR where applicable, and internal policies.

Where possible, data should be minimised, anonymised, or de-identified to reduce risk.

Users must recognise that some information may be stored in cloud or external systems and take appropriate precautions.

6. Roles and Responsibilities

6.1 Executive Management - approve this policy, oversee implementation, and provide resources for security initiatives.

6.2 Information Security Officer / IT Security Team - implement and monitor controls, support incident management.

6.3 Data Owners - define classification, retention, and access requirements for information under their control

6.4 All Users - follow this policy, report incidents, and protect information assets under their control





7. Policy Compliance

7.1 Compliance Measurement

Compliance with this policy may be verified through reviews, audits, system monitoring, and management oversight.

7.2 Exceptions

Any exception to this policy must be approved in advance by management.

7.3 Non-Compliance

Any individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or engagement.

8. Related Standards, Policies and Processes

- Privacy Policy
- Information Security Policy
- Incident Response Policy

9. Revision History

None.

