**Information Security Policy**

<Logo here>

**Your Organisation’s Name**

ABN or another Organisation Identifier

Your Organisation’s Website

Table of Contents

[1. Purpose 3](#_Toc196778579)

[2. Scope 3](#_Toc196778580)

[3. Definitions 3](#_Toc196778581)

[4. Roles and Responsibilities 4](#_Toc196778582)

[5. Information Security Objectives 4](#_Toc196778583)

[6. Security Principles 5](#_Toc196778584)

[7. Control Areas 5](#_Toc196778585)

[8. ISMS Integration 5](#_Toc196778586)

[9. Information Security in Project Management 6](#_Toc196778587)

[Policy Exception 6](#_Toc196778588)

[Policy Violation 6](#_Toc196778589)

[References 7](#_Toc196778590)

[Document Control 7](#_Toc196778591)

[Revision 8](#_Toc196778592)

[Revision History 8](#_Toc196778593)

# Purpose

Organisation is <a succinct introduction of the Organisation with a focus on information handling>

Organisation is committed to protecting the confidentiality, integrity, and availability of its information assets. This policy sets out how information security is managed to reduce risks, ensure compliance with relevant regulatory obligations, and align with the ISO/IEC 27001:2022 standard.

# Scope

This policy applies to:

* All employees, contractors, consultants, and third-party providers with access to Organisation’s information assets
* All information, systems, devices, networks, and services used for business purposes
* All work environments (onsite, remote, cloud, on-premises, or hybrid)

# Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| BCP | Business Continuity Plan |
| Designated Security Lead | The internal role or outsourced provider responsible for implementing security measures |
| Information Asset | Any data, device, system, or process that stores or processes information |
| ISMS | Information Security Management System, a structured framework for managing security risks |
| KPIs | Key Performance Indicators |
| MFA | Multi-Factor Authentication |
| MSP | Managed Service Provider |
| Staff | All employees, contractors, consultants, and other personnel with access to Organisation’s information and information systems |

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| All Users | Comply with this policy, complete training, report incidents or concerns |
| Managers | Reinforce policy, support secure practices within teams |
| Designated Security Lead (or MSP) | Maintain the ISMS, coordinate audits, lead risk and incident response |
| Third Parties | Meet agreed security controls, report incidents, protect Organisational data |

*ITPL.003 Information Security Roles and Responsibilities* document lists detailed information security related roles and responsibilities across the Organisation.

# Information Security Objectives

The following information security objectives support Organisation’s commitment to managing information risks effectively, maintaining trust with stakeholders, and complying with legal and regulatory requirements. These objectives apply across all systems, environments, and functions, and guide the implementation and continuous improvement of security controls throughout the Organisation.

|  |  |
| --- | --- |
| **Objective** | **Implementation** |
| Manage risks | Maintain and review risk register; implement controls to reduce identified risks |
| Control access | Enforce least privilege, MFA, and access reviews |
| Protect sensitive data | Classify data; apply encryption, retention, and secure disposal controls |
| Ensure business continuity | Maintain backup schedules, test restoration, document BCP |
| Detect/respond to threats | Log key events; respond to alerts; escalate incidents per documented procedures |
| Support awareness | Deliver onboarding and refresher training annually |
| Manage supplier risk | Vet vendors; include security clauses in contracts; reassess at least annually |
| Maintain compliance | Track obligations; update policies in response to legal or contractual change |

# Security Principles

The following principles guide all security efforts:

* **Defence-in-depth**: Multiple layers of controls to prevent and detect incidents
* **Least privilege**: Staff are granted only the access needed to perform their roles
* **Secure-by-default**: Systems and services should default to secure configurations
* **Accountability**: All actions must be attributable and reviewable
* **Compliance**: Legal, regulatory, and contractual obligations must be met
* **Continual improvement**: Security controls and awareness evolve over time

# Control Areas

Organisation maintains supporting controls, standards, or procedures covering:

* **Access Control**
* **Device Security**
* **Data Protection**
* **Third-Party Management**
* **Monitoring and Logging**
* **Incident Response**
* **Business Continuity**
* **Secure Development**(if applicable)
* Regulatory Compliance

# ISMS Integration

This policy is part of Organisation’s ISMS aligned to ISO/IEC 27001:2022. Supporting elements of the ISMS include:

* Statement of Applicability (SoA)
* ISMS Scope Statement
* Information Security Risk Management Framework
* Internal Audit and Management Review processes
* Other relevant ISMS policies and procedures

# Information Security in Project Management

Information security requirements must be identified, assessed, and incorporated into all projects from initiation through to completion. Project risk assessments must include security considerations aligned to Organisation’s ISMS.

Project managers must ensure that information security is considered during project initiation, planning, execution, and closure. Security risk assessments must be completed for new projects, significant changes, and procurement activities impacting information assets or infrastructure.

Project deliverables must be reviewed for compliance with Organisation’s security standards before handover to operations.

# Policy Exception

Requests for exceptions to this policy must be submitted in writing to the Designated Security Lead. Each request must include a clear business justification, risk assessment, and mitigation plan. Approved exceptions must be time-bound and reviewed periodically.

# Policy Violation

Violations of this policy, or of supporting information security policies and procedures, may result in disciplinary action up to and including termination of employment or contract. Serious breaches may also be referred to regulatory authorities where legally required.

All identified or suspected violations must be reported promptly to the Staff member’s Manager and the the Designated Security Lead. The Designated Security Lead, in coordination with HR and Legal as appropriate, will assess the violation and determine corrective and disciplinary actions based on the severity and impact of the breach.

# References

This policy should be read in conjunction with the following supporting documentation:

* ISO/IEC 27001:2022 Information Security Management Standard
* ISO/IEC 27001:2022 Statement of Applicability (SoA)
* Supporting information security policies and procedures

# Document Control

| Policy Contact | [Designated Security Lead or Role] |
| --- | --- |
| Policy Owner | [Designated Security Lead or Role] |
| Approved by | [Approver] |
| Date of Approval | [Insert Date] |
| Next Review Date | [Date of Approval + 12 Months] |
| ISO 27001:2022 Reference | * C5.1 Leadership and commitment
* C5.2 Policy
* A5.1 Policies for Information Security
* A5.8 Information security in project management
 |

# Revision

This policy will be reviewed at least annually, or following:

* Significant security incidents
* Changes to business operations or technology
* Updates to applicable legal or regulatory obligations

The Designated Security Lead is responsible for ensuring the policy’s continued relevance and effectiveness.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Description | Date |
| V1.0  | TBD | Initial version | [Insert Date] |
| V1.1 | TBD | Reviewed and approved | [Insert Date] |