Information Security Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides a foundation for information security governance. Your specific security requirements will depend on your industry, data types and risk profile. Consider engaging IT security professionals for implementation guidance.

1. Purpose

This policy establishes [Company Name]'s commitment to protecting information assets from threats, whether internal or external, deliberate or accidental. It defines the framework for managing information security across the organisation.

2. Scope

This policy applies to:

- All employees, contractors, and third parties with access to company information
- All information assets regardless of format or location
- All IT systems, networks and applications
- All business processes that create, store, process or transmit information

3. Information Security Objectives

[Company Name] is committed to:

- Protecting information from unauthorised access (Confidentiality)
- Ensuring information is accurate and complete (Integrity)
- Ensuring information is accessible when needed (Availability)
- Complying with legal and regulatory requirements
- Building security awareness across the organisation

4. Information Classification

4.1 Classification Levels

[Company Name] uses the following classification levels:

- Public: Information that can be freely shared
- Internal: Information for internal use only
- Confidential: Sensitive business information

- Restricted: Highly sensitive information with limited access

4.2 Handling Requirements

Each classification level has specific handling requirements covering:

- Storage and transmission
- Access controls
- Sharing restrictions
- Disposal methods

5. Access Control

5.1 Access Principles

- Access granted on a need-to-know basis
- Principle of least privilege applied
- Access rights reviewed regularly
- Segregation of duties where appropriate

5.2 User Access Management

- Formal user registration and deregistration process
- Unique user IDs for accountability
- Regular access reviews
- Prompt removal of access when no longer required

5.3 Authentication

- Strong password requirements
- Multi-factor authentication for sensitive systems
- Account lockout after failed attempts
- Regular password changes

6. Physical Security

- Secure areas for sensitive information processing
- Access controls to work areas
- Visitor management procedures
- Clean desk and clear screen policy
- Secure disposal of paper documents
- Protection of equipment from environmental threats

7. IT Security

7.1 Network Security

- Firewall protection
- Network segmentation where appropriate
- Secure wireless configurations
- Intrusion detection/prevention
- Secure remote access

7.2 System Security

- Regular security patching
- Antivirus and anti-malware protection
- Secure system configurations
- Regular vulnerability assessments

7.3 Application Security

- Secure development practices
- Security testing before deployment
- Regular application updates

8. Data Security

8.1 Data Protection

- Encryption of sensitive data at rest and in transit
- Secure backup procedures
- Data loss prevention measures
- Secure data disposal

8.2 Backup and Recovery

- Regular backups of critical data
- Offsite or cloud backup storage
- Regular backup testing
- Documented recovery procedures

9. Mobile and Remote Working

- Secure mobile device configurations
- VPN use for remote access
- BYOD requirements where applicable
- Physical security of devices when remote
- Secure handling of sensitive information

10. Third-Party Security

When engaging third parties with access to information:

- Security requirements in contracts
- Due diligence on security practices
- Appropriate confidentiality agreements
- Regular monitoring of compliance
- Secure data sharing mechanisms

11. Incident Management

11.1 Incident Reporting

- All security incidents must be reported promptly
- Report to [IT/Security Manager]
- Do not attempt to investigate without authorisation
- Preserve evidence

11.2 Incident Types

- Unauthorised access or access attempts
- Malware infections
- Data breaches or loss
- Physical security incidents
- Policy violations

11.3 Incident Response

- Documented incident response procedures
- Containment and recovery actions
- Root cause analysis
- Lessons learned and improvements

12. Business Continuity

- Business continuity plans for critical systems
- Disaster recovery procedures
- Regular testing of plans
- Alternative processing arrangements

13. Compliance

[Company Name] will comply with:

- Privacy Act 1988 and Australian Privacy Principles

- Industry-specific regulations
- Contractual security requirements
- Relevant security standards and frameworks

14. Security Awareness

- Security awareness training for all staff
- Induction training on security policies
- Regular updates on security threats
- Ongoing security reminders

15. Responsibilities

15.1 All Staff

- Comply with security policies
- Report security incidents
- Complete required training
- Protect information assets

15.2 Management

- Ensure team compliance
- Support security initiatives
- Lead by example

15.3 IT/Security Team

- Implement security controls
- Monitor security status
- Respond to incidents
- Maintain security documentation

16. Policy Breaches

Breaches of this policy may result in:

- Disciplinary action
- Revocation of access
- Termination of employment
- Legal action for serious breaches

17. Review

This policy will be reviewed:

- At least annually

- After security incidents
- When threats or technology change significantly
- When business requirements change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Information Security Policy. I understand my responsibilities for protecting information assets and agree to comply with this policy.

Employee Name: _____

Signature: _____

Date: _____