Data Protection & Confidentiality Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides general guidance on data protection and confidentiality. Organisations handling personal information must comply with the Privacy Act 1988 and Australian Privacy Principles. Seek legal advice for specific compliance requirements.

1. Purpose

This policy establishes how [Company Name] collects, uses, stores and protects confidential information and personal data. It ensures compliance with the Privacy Act 1988 and the Australian Privacy Principles (APPs), while protecting the interests of our employees, customers and business partners.

2. Scope

This policy applies to:

- All employees, contractors and third parties with access to company information
- All forms of confidential and personal information
- Information in any format (electronic, paper, verbal)
- All business operations and locations

3. Definitions

3.1 Personal Information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not.

3.2 Sensitive Information

A subset of personal information that includes:

- Health information
- Racial or ethnic origin
- Political opinions or membership
- Religious beliefs or affiliations
- Sexual orientation or practices

- Criminal record
- Biometric information

3.3 Confidential Information

Business information that is not publicly available, including:

- Trade secrets and intellectual property
- Financial information
- Business strategies and plans
- Customer and supplier lists
- Pricing and contract information
- Employee records

4. Data Collection

4.1 Collection Principles

[Company Name] will only collect personal information that is:

- Necessary for our functions or activities
- Collected by lawful and fair means
- Collected directly from the individual where practicable

4.2 Notification

When collecting personal information, we will inform individuals about:

- Our identity and contact details
- The purposes of collection
- Who the information may be disclosed to
- How to access and correct information
- Consequences if information is not provided

5. Data Use and Disclosure

5.1 Use Limitations

Personal information will only be used or disclosed for:

- The primary purpose for which it was collected
- A secondary purpose the individual would reasonably expect
- Purposes with individual consent
- Purposes required or authorised by law

5.2 Disclosure Restrictions

- Information is disclosed on a need-to-know basis
- Third-party disclosures require appropriate agreements

- Cross-border disclosure must meet APP requirements
- Marketing use requires consent

6. Data Storage and Security

6.1 Storage Requirements

- Store data securely with appropriate access controls
- Use encryption for sensitive electronic data
- Secure physical storage for paper records
- Regular backup of electronic data
- Clear desk and clear screen practices

6.2 Retention

- Retain data only for as long as necessary
- Follow legal retention requirements
- Securely destroy data when no longer needed
- Maintain retention schedules

7. Data Quality

[Company Name] will take reasonable steps to ensure personal information is:

- Accurate and up-to-date
- Complete and relevant
- Not misleading

Individuals should notify us of any changes to their information.

8. Access and Correction

8.1 Access Rights

Individuals have the right to:

- Request access to their personal information
- Receive access within a reasonable timeframe
- Be given reasons if access is denied

8.2 Correction Rights

- Request correction of inaccurate information
- Have corrections made within a reasonable timeframe
- Request a statement be attached if correction is refused

9. Confidentiality Obligations

9.1 Employee Obligations

All employees must:

- Treat confidential information with care
- Only access information required for their role
- Not disclose confidential information without authorisation
- Not use confidential information for personal benefit
- Report suspected breaches immediately

9.2 Ongoing Obligations

- Confidentiality obligations continue after employment ends
- Return all confidential information when leaving
- Do not retain copies of confidential information

10. Data Breach Response

10.1 Identifying Breaches

A data breach occurs when personal information is:

- Accessed without authorisation
- Disclosed to unauthorised parties
- Lost or stolen
- Altered without authorisation

10.2 Reporting Breaches

- Report suspected breaches immediately to [designated person]
- Do not attempt to investigate without authorisation
- Preserve evidence
- Cooperate with investigations

10.3 Notifiable Data Breaches

Under the Notifiable Data Breaches scheme, [Company Name] must notify the OAIC and affected individuals if a breach is likely to result in serious harm.

11. Third-Party Management

When engaging third parties with access to personal information:

- Conduct due diligence on data handling practices
- Include appropriate confidentiality clauses in contracts
- Monitor compliance with requirements

- Ensure data is returned or destroyed at end of engagement

12. Training and Awareness

- All employees receive data protection training
- Training is provided during induction
- Regular refresher training is conducted
- Awareness of current threats and risks

13. Responsibilities

13.1 All Employees

- Handle data according to this policy
- Report breaches and concerns
- Complete required training
- Maintain confidentiality

13.2 Management

- Ensure team compliance
- Approve access to confidential information
- Support policy implementation

13.3 Privacy Officer

- Oversee policy compliance
- Handle privacy inquiries and complaints
- Manage data breach responses
- Coordinate with the OAIC as required

14. Compliance and Breaches

Breaches of this policy may result in:

- Disciplinary action up to and including termination
- Legal action for serious breaches
- Reporting to relevant authorities
- Civil liability for damages

15. Review

This policy will be reviewed:

- At least annually
- When privacy laws change
- After significant data incidents

- When business practices change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Data Protection & Confidentiality Policy. I understand my obligations and agree to comply with all requirements for handling confidential and personal information.

Employee Name: _____

Signature: _____

Date: _____