Artificial Intelligence (AI) Policy

[Company Name] Managed Service Provider

Document Owner: Managing Director / CTO **Approved By:** Board / Executive **Version:** 0.1 **Review Cycle:** 6 Monthly **Next Review Date:** [Insert Date]

1. Purpose

This policy establishes how Artificial Intelligence systems are selected, implemented, governed and monitored within [Company Name] (“the Company”).

It ensures AI is used responsibly, securely and in alignment with legal, ethical and commercial obligations to customers.

2. Scope

This policy applies to:

- All employees, contractors and consultants
- All AI systems used internally
- All AI-enabled services delivered to customers
- All integrations involving third-party AI providers
- All data processed through AI systems

This includes but is not limited to:

- Generative AI tools (e.g. ChatGPT, Copilot, Claude)
- AI-enabled cybersecurity tools
- AI-driven automation platforms
- Predictive analytics systems
- AI embedded in vendor products

3. Definitions

Artificial Intelligence (AI): Software systems capable of performing tasks that typically require human intelligence.

High-Risk AI: AI systems that materially affect legal rights, financial decisions, security posture, employment outcomes, or regulatory compliance.

Customer Data: Any data belonging to customers, including personal, confidential or commercially sensitive information.

4. Guiding Principles

The Company adopts the following principles:

1. **Security First** – No AI system may compromise customer or company data.

2. **Human Oversight** – AI supports decision-making, it does not replace accountability.
3. **Transparency** – Customers must be informed when AI materially impacts service delivery.
4. **Compliance** – AI must comply with Australian law including Privacy Act 1988, APPs and relevant industry standards.
5. **Risk Proportionality** – Controls scale with risk level.

5. Governance Structure

Role	Responsibility
Board / Executive	Oversight of AI strategy and risk
CTO / Technical Director	AI tool approval and architecture governance
Security Officer	Data protection and risk assessment
Service Delivery Manager	Operational monitoring
All Staff	Responsible use and reporting concerns

An AI Register shall be maintained documenting:

- AI tool name
- Vendor
- Data classification processed
- Risk rating
- Approval status
- Review date

6. AI Use Categories

6.1 Approved Low-Risk Use

- Drafting documentation
- Code assistance
- Internal knowledge summarisation
- Marketing content drafting

No customer confidential data may be entered into public AI tools unless:

- Covered by a commercial agreement
- Data processing terms reviewed
- Data residency assessed

6.2 Moderate-Risk Use

- AI-assisted ticket triage
- Log analysis
- Reporting automation
- Chatbots interacting with customer users

Requires:

- Risk assessment
- Security review
- Customer notification if applicable

6.3 High-Risk Use

- Automated decision-making affecting security posture
- Financial forecasting
- Identity verification
- HR decision support

Requires:

- Formal Risk Assessment
- Executive approval
- Legal review (if required)
- Audit logging enabled

7. Data Handling Requirements

7.1 Data Classification

AI systems may only process data appropriate to their approved classification level.

7.2 Prohibited Data

Unless specifically approved:

- Full financial records
- Health records
- Sensitive personal information
- Credentials or API keys

7.3 Data Residency

Where possible, AI systems should operate within Australian data centres or approved jurisdictions.

8. Vendor Due Diligence

Before onboarding an AI vendor, the following must be assessed:

- Security certifications (ISO 27001, SOC 2, etc.)
- Data retention policy
- Model training data practices
- Sub-processors
- Incident response capability
- Right to audit (where applicable)

9. Security Controls

All AI systems must:

- Enforce role-based access control
- Log user activity
- Prevent prompt injection vulnerabilities where possible
- Use secure API authentication
- Have data loss prevention controls where feasible

10. Human Oversight & Quality Control

AI outputs must:

- Be reviewed before customer delivery
- Not be relied upon blindly
- Be verified when impacting security, legal or financial outcomes

The Company does not represent AI outputs as professional advice without human validation.

11. Customer Transparency

Where AI materially affects customer service delivery:

- Customers shall be informed
- Limitations shall be disclosed
- Data processing terms clarified

AI use shall not contradict contractual obligations.

12. Incident Management

If an AI-related incident occurs:

1. Contain the issue
2. Notify Security Officer
3. Assess data impact
4. Follow breach notification obligations
5. Update risk register

All AI incidents must be documented.

13. Staff Training

All staff must:

- Complete annual AI awareness training
- Understand risks of data leakage
- Understand prompt injection and social engineering risks
- Know escalation pathways

14. Shadow AI

Unauthorised AI tool usage is prohibited.

Staff must not:

- Upload customer data into unapproved AI systems
- Integrate AI tools without approval
- Use personal AI accounts for company work

15. Monitoring & Review

The AI Register and risk ratings will be reviewed:

- Every 6 months
- After any major AI incident
- After major regulatory change

16. Compliance & Regulatory Alignment

This policy aligns with:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- ACSC Essential Eight
- ISO 27001 (where applicable)
- Contractual obligations to customers

17. Breach of Policy

Failure to comply with this policy may result in:

- Disciplinary action
- Termination of employment or contract
- Legal consequences where applicable

Optional Appendices

Appendix A – AI Risk Assessment Template

- AI Tool Name
- Business Purpose
- Data Types Processed
- Risk Level (Low/Medium/High)
- Security Controls in Place
- Vendor Assessment Completed
- Executive Approval (if required)

Appendix B – AI Use Disclosure Clause for MSP Agreements

"The Service Provider may utilise Artificial Intelligence systems to assist in service delivery. Such systems operate under human oversight and comply with applicable privacy and data protection obligations."