Privacy and Security Management Plan

Version 1.0	Updated 09/09/2025	Next review 09/09/2026

1. Purpose

This plan operationalises Marco Polo Portal's Privacy & Security Policy by setting out specific actions, responsibilities, and performance indicators to ensure compliance with the **Privacy Act 1988 (Cth)**, the **Australian Privacy Principles (APPs)**, and the **NDIS Practice Standards**.

2. Objectives & Actions

Objective	Action Steps	Performance Indicators / KPIs	Responsibility	Timeline
Ensure Legal & Regulatory Compliance	Monitor compliance with the Privacy Act, APPs, NDIS Act, and Practice Standards. Maintain up-to-date Privacy & Security Policy. Embed privacy into procurement and contracting.	100% policy reviews completed annually. All supplier contracts include privacy & data security clauses. Zero compliance breaches reported.	Privacy Officer + Board	Annual

Protect Personal & Sensitive Information	Encrypt data at rest and in transit. Apply role-based access controls. Implement multi-factor authentication (MFA).	100% data encrypted. Access logs reviewed quarterly. MFA required for 100% of staff with system access.	IT Lead + Privacy Officer	Ongoing
Strengthen Cybersecurity Posture	Conduct penetration testing and vulnerability scans. Apply timely security patches and updates. Monitor for suspicious activity.	Annual penetration test completed. Critical vulnerabilities remediated within 30 days. Security incidents < 2 per year.	IT Lead	Quarterly
Data Minimisation & Retention	Collect only information necessary for service delivery. Apply retention schedules for NDIS participant data. Securely destroy records once retention period ends.	100% records reviewed against retention schedules annually. Evidence of certified secure destruction.	Privacy Officer + HR	Annual

Respond to Data Breaches	Maintain a breach response protocol in line with the Notifiable Data Breaches Scheme. Train staff on incident reporting. Notify OAIC and NDIS Commission when required.	100% breaches reported within statutory timelines. 100% staff trained in reporting protocols annually.	Privacy Officer + IT Lead	Ongoing
Staff Training & Awareness	Deliver annual privacy and cybersecurity training. Include privacy induction for new staff. Provide refresher modules on phishing, confidentiality, and NDIS privacy standards.	100% of staff trained annually. 90%+ pass rate on knowledge checks. Training completion recorded in HR system.	HR + Privacy Officer	Annual

Participant Rights & Transparency	Provide clear privacy notices to all users. Enable access and correction requests. Respond promptly to privacy complaints.	100% privacy requests acknowledged within 5 business days. 100% complaints resolved within 30 days. Privacy notice published on website and platform.	Privacy Officer	Ongoing
Governance & Continuous Improvement	Quarterly reporting to the Board. Annual independent audit of privacy and security controls. Benchmark practices against ISO 27001 standards.	4 Board reports delivered annually. Annual audit completed. Continuous improvement actions implemented within 3 months.	Board + Privacy Officer	Quarterly + Annual

3. Governance & Accountability

- **Board of Directors** – ultimate accountability for privacy and security.
- **Privacy Officer** – responsible for compliance, breach reporting, and monitoring.
- **IT Lead** – responsible for cybersecurity, system controls, and monitoring.
- **Managers** – ensure team compliance with privacy obligations.
- **All Employees & Contractors** – required to comply with privacy and security policies and complete training.

4. Incident Response Process

1. **Identify** – suspected data breach or privacy issue reported immediately.
2. **Contain** – IT and Privacy Officer act to contain breach.
3. **Assess** – determine if breach is likely to result in serious harm (APP 11 & NDB Scheme).
4. **Notify** – if required, notify OAIC, NDIS Commission, and affected individuals within statutory timeframes.
5. **Review** – implement corrective measures and update processes.

5. Participant Access & Control

- Participants may access their information by written request.
- Requests are verified for identity before access is granted.

- Corrections are made within **30 days** of a valid request.
- Consent can be withdrawn at any time unless required by law.

6. Monitoring & Reporting

- **Quarterly** internal review of access logs, security alerts, and privacy complaints.
- **Annual** independent privacy and security audit.
- De-identified metrics reported to the Board, including:
    - Number of access requests.
    - Number of complaints received and resolved.
    - Number of data breaches (if any).

7. Review & Continuous Improvement

- This plan will be reviewed annually by the Privacy Officer and Board.
- Targets will be progressively raised as Marco Polo Portal scales.
- Lessons learned from audits, incidents, and sector best practice will inform updates.

8. References

- Privacy Act 1988 (Cth) & Australian Privacy Principles
- Notifiable Data Breaches (NDB) Scheme
- NDIS Act 2013 (Cth)
- NDIS Code of Conduct
- NDIS Practice Standards (Privacy & Dignity; Information Management)
- Office of the Australian Information Commissioner (OAIC) Guidelines
- ISO 27001 Information Security Management
-

Approved by:

Board of Directors, Marco Polo Portal
Date: 09/09/2025