Information Management and Privacy Policy

1. Purpose

The purpose of this Information Management and Privacy Policy is to establish a comprehensive framework for the management of information at AT Resolutions. This policy ensures that information is handled in a secure, compliant, and efficient manner while safeguarding the privacy of all stakeholders. It aligns with the National Disability Insurance Scheme (NDIS) Standards, as well as relevant privacy and data protection regulations.

2. Scope

This policy applies to all employees, contractors, consultants, and third-party service providers who have access to information managed by AT Resolutions. It covers all forms of information including digital, physical, personal, operational, and confidential data collected, stored, processed, or transmitted by the company.

3. Definitions

- Information Management: The processes, systems, and policies used to gather, store, process, and distribute information within an organisation.
- Privacy: The right of individuals to control the collection, use, and disclosure of their personal information.
- Personal Information: Information about an identifiable individual that is collected, processed, or stored by the business.
- Sensitive Information: Information that is considered sensitive under privacy law, including health records, racial or ethnic origins, and other private details.
- NDIS Information: Any data related to a participant in the National Disability Insurance Scheme (NDIS), including personal, health, and service-related information.

4. Information Management Framework

AT Resolutions will establish and maintain an integrated information management system that covers the following key principles:

1. Confidentiality: Information will be accessed only by authorised personnel and will be protected from unauthorised access, alteration, or disclosure.
2. Integrity: Information will be accurate, reliable, and up-to-date, and will be regularly reviewed for consistency and relevance.
3. Availability: Information will be accessible when required, and procedures will be in place to ensure prompt access to information during business operations.
4. Compliance: Information management practices will comply with applicable Australian laws, including the Privacy Act 1988 (Cth), the NDIS Act 2013, and the NDIS Quality and Safeguarding Framework.
5. Transparency: Stakeholders will be informed of how their information is used and processed, and how they can access, correct, or request the deletion of their data.

5. Privacy and Data Protection

AT Resolutions is committed to protecting the privacy of its clients, employees, and partners. The following practices will be implemented to ensure compliance with the Privacy Act 1988 and other applicable privacy laws:

1. Data Collection: Personal and sensitive information will only be collected for specific, lawful purposes and with the consent of the individual where required. Information collected for NDIS participants will adhere to the NDIS Practice Standards and Quality Indicators.
2. Data Storage: All personal and sensitive data will be securely stored in both physical and digital formats. Digital data will be encrypted, and physical records will be stored in locked facilities. Access to stored data will be strictly controlled and monitored.
3. Data Use: Personal data will only be used for the purposes for which it was collected, and any use beyond the original purpose will be subject to further consent. NDIS data will be used in accordance with the participant's NDIS service agreement.
4. Data Sharing: Data will only be shared with third parties when necessary and with the explicit consent of the individual concerned, except where required by law or regulation. NDIS data sharing will comply with the NDIS Code of Conduct and Privacy Principles.
5. Data Retention and Disposal: Personal and sensitive data will be retained only for as long as required by law or business need. Once the retention period has expired, data will be securely destroyed or anonymised.
6. Data Breaches: Any data breaches will be reported and handled in compliance with the Privacy Act and the Notifiable Data Breaches (NDB) scheme. The company will investigate any breaches promptly, notify affected parties, and implement corrective actions.

6. Information Access and Security

1. Access Control: Access to information will be limited to authorised personnel only. All users must be authenticated before accessing any sensitive or personal information. Access controls will be enforced through password protection, multi-factor authentication, and role-based permissions.
2. Physical Security: Physical access to information storage areas (both digital and paper records) will be restricted to authorised personnel only. Secure access controls such as locked cabinets and secure rooms will be used.
3. Cybersecurity: All digital information will be protected by up-to-date cybersecurity measures, including firewalls, anti-malware software, and intrusion detection systems. Regular security audits will be conducted to assess vulnerabilities and implement necessary improvements.
4. Employee Training: Employees and contractors will be provided with regular training on data protection, information management, and privacy principles. This training will cover handling sensitive information, reporting data breaches, and complying with the NDIS Standards.

7. NDIS Compliance

As a provider of services to NDIS participants, AT Resolutions will adhere to the following:

1. NDIS Participant Rights: AT Resolutions will ensure that all NDIS participants are fully informed of their rights regarding the collection, storage, and sharing of their personal

information. Participants will be given clear options to consent or withdraw consent to data collection.

2. NDIS Participant Data Management: NDIS participant data will be handled in accordance with the NDIS Practice Standards and Quality Indicators. Specific attention will be given to confidentiality, accuracy, and accessibility of NDIS-related records.
3. Incident Reporting: Any incidents involving NDIS participant data that may result in harm, including breaches of confidentiality, will be reported to the NDIS Quality and Safeguards Commission and managed according to the NDIS Incident Management and Reporting guidelines.

8. Responsibilities

1. Management: Senior management will ensure the overall implementation of this policy and will allocate resources necessary for compliance and effectiveness.
2. Data Protection Officer (DPO): A designated Data Protection Officer (DPO) will be responsible for overseeing the company's information management and privacy practices. The DPO will ensure compliance with this policy and handle any data privacy concerns or breaches.
3. Employees and Contractors: All employees and contractors are required to follow the information management and privacy practices outlined in this policy. They must report any concerns or breaches promptly to the DPO.

9. Policy Review and Updates

This policy will be reviewed annually or as required by changes in legislation or business needs. Any updates to the policy will be communicated to all relevant parties, and necessary training will be provided.

10. Non-Compliance

Failure to comply with this policy may result in disciplinary action, including termination of employment or contract. Legal action may also be taken if non-compliance results in a breach of privacy laws.

11. Approval

This Information Management and Privacy Policy is approved by the Board of AT Resolutions and is effective as of 1st July 2025.