Records Retention & Destruction Policy:

Privacy, Security, Retention and Destruction of Business Information

Last Update: 26/04/2026
Version: 1.2

RUNPAY™ DISCLAIMER: This Policy Framework is provided in good faith and intent for Business Owners and Executives of Australia. It is based on common Australian standards but is not a customised Legal document, nor does it constitute Legal Advice to any user of it. *The Law varies depending on your specific circumstances/Jurisdiction and using or adapting this Policy does not create any Lawyer-Client relationship with RUNPAY™*. **Any Business Owner using this template should always seek independent Legal Advice from a Qualified Australian Lawyer before relying on, signing or using any detail provided within this Policy**. RUNPAY™ makes no warranties or representations about the suitability, accuracy, completeness or currency of this Policy (or any third-party services) for your particular situation. **Use is entirely at your own risk**.

Policy Statement

This Policy sets out the Framework for the creation, storage, retention, security, privacy, use and secure Destruction of all Business Records and Information *(Physical and Electronic)*.

Its purpose is to:
(a) ensure necessary records and documents are adequately protected and maintained;
(b) ensure unneeded records or those of no value are discarded at the appropriate time; and
(c) comply with all applicable Legislative requirements.

Effective protection of Business information creates a competitive advantage by preserving the Businesses reputation and reducing the risk of negative events and incidents. This Policy balances Legislative requirements, Confidentiality of data and documents, integrity of IT systems, Reputation as a Trusted Recipient of Data and reliable storage and Back-up systems.

This Policy applies Australia-wide to all Workers (Employees, Independent Contractors, Directors, Volunteers and Vendors) and to all records in any format — hardcopies, electronic files (emails, databases, spreadsheets etc.), portable devices and any other media containing Business, Employee, Client, Worker or any other confidential information. In any situation, Queensland Rules take priority where they impose additional or stricter requirements than National Standards.

This Policy will be reviewed annually in January OR after any significant Legislative or Business Process change. The Disposal of Records Activity occurs in December each year.

1. Legislative Framework

Our Practices comply with the following Legislation, Regulations, Codes of Practice and Standards (as amended or replaced from time to time). *Queensland-specific rules take priority where they are additional or stricter than National equivalents.*

National / Harmonised Laws

- *Privacy Act 1988 (Cth)* and the 13 *Australian Privacy Principles (APPs)*, particularly *APP 11* (Security of Personal Information and Destruction / De-identification when no longer needed).
- *Notifiable Data Breaches (NDB) scheme* – mandatory notification to the OAIC and affected individuals.
- *Fair Work Act 2009 (Cth)* and *Fair Work Regulations* (Employee Records).
- *Corporations Act 2001 (Cth)* and ATO requirements (Financial and Tax Records).
- *Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model* (Maturity Level 1 recommended).
- *National Disability Insurance Scheme Act 2013 (Cth)*, *NDIS Practice Standards*, *NDIS (Incident Management and Reportable Incidents) Rules 2018*, and *NDIS Code of Conduct* (where the Business delivers NDIS supports).
- *Disability Discrimination Act 1992 (Cth)* (DDA) – Reasonable Adjustments and Non-Discrimination in Employment.

Queensland-Specific Rules (Priority Where Stricter Rules Apply)

- *Work Health and Safety Act 2011 (Qld)* and *Work Health and Safety Regulation 2011 (Qld)* (or equivalent harmonised model WHS Laws in other Jurisdictions).
- Applicable Codes of Practice issued by the Regulator, including:
    - *Managing the Risk of Psychosocial Hazards at Work Code of Practice 2022 (Qld)* / Model Code (*Safe Work Australia*, with updates including the *2024 Commonwealth version* where applicable);
    - *Managing the Work Environment and Facilities Code of Practice 2021*;
    - *First Aid in the Workplace Code of Practice 2021*;
    - *How to Manage Work Health and Safety Risks Code of Practice 2021*;
    - Framework for Alcohol and Drug Management in the Workplace;
    - *Work Health and Safety (Sexual and Gender-based Harassment) Code of Practice 2025*.
- *Workers' Compensation and Rehabilitation Act 2003 (Qld)* (WCRA) administered by WorkCover Queensland (primary Jurisdiction) and equivalent legislation in other States/Territories. The Business meets all obligations for claim notification, Injury Management, Rehabilitation and Return-to-Work programs.

Anti-Discrimination and Other Legislation

- *Sex Discrimination Act 1984 (Cth)*, *Anti-Discrimination Act 1991 (Qld)* and other Federal and State Laws prohibiting Discrimination on protected attributes and imposing positive duties to prevent unlawful conduct (including Sexual Harassment and Sex-based Harassment).
- *Tobacco and Other Smoking Products Act 1998 (Qld)* (and equivalents in other Jurisdictions).

If the Business is located across multiple Jurisdictions, the most stringent requirement always applies.

2. Scope

This Policy applies Australia-wide to all Workers (Employees, Independent Contractors, Volunteers, Vendors and Directors) and to all records in any format — hardcopies, electronic files (emails, databases, spreadsheets etc.), portable devices and any other media containing Business, Employee, Client, Worker or any other confidential information. This Policy applies equally to ALL Work performed from Home, Remotely or when using a Personal Device.

3. Employee Privacy

The Business takes its obligations under the *Privacy Act 1988 (Cth)* seriously when handling Worker personal information.

Personal Information We Collect

We collect personal information relating to your:

- Recruitment, performance, discipline and ending of employment;
- Terms and conditions of employment;
- Personal contact details, hours of work, remuneration, leave and superannuation;
- Health or personal circumstances where relevant to your role or safety;
- Records created or accessed using Business equipment or systems (computers, internet, email, phones); and
- Any other information provided, from time-to-time, by you to the Business.

Purpose and Management

This information is collected to manage your engagement with the Business and meet Legal obligations. It is stored securely and retained in accordance with the *Records Retention Schedule* in **Section 5** of this Policy.

Access and Correction
You may request access to or correction of your personal information by contacting the **Delegated Business Leader** (for Privacy/Security).

Employee Obligations
You must treat all personal information of Clients and other Workers confidentially and in accordance with the *Privacy Act* and this Policy. Breaches may result in disciplinary action, up to and including termination.

Further Information
For more details on how we handle all Business records and information (including Worker's records), refer to the rest of this Policy, particularly **Section 5** (Storage), **Section 6** (Security Controls), **Section 8** (Destruction), and **Section 11** (Incident Reporting).

4. Responsibilities

All individuals specified within Section 2 (**Scope**) must comply with it unless otherwise specified in writing by the appropriate **Delegated Business Leader**. Where in doubt about Security, Privacy, Retention or Destruction, take a cautious approach and seek advice immediately. The **Delegated Business Leader** (for Privacy/Security) is responsible for overall implementation, monitoring, training, breach response and compliance. A **Delegated Business Leader** (for Document Control) supports day-to-day retention, scheduling of Record Destruction and Legal Holds. Contact details are located within the **Business Delegations** document. *All individuals with access to Business records must follow a need-to-know basis when sharing information or granting access to Business information.*

5. Records Retention Schedule

All records must be retained for the *longest applicable period* required by Law, Regulation, Contract or Business needs. Where multiple requirements overlap, the longest period applies. Records must be kept in a legible form, be readily accessible, accurate and not altered except to correct errors.

Record Category	Minimum Retention Period	Key Legislation / Regulator	Compliance Requirements & Additional Notes
Tax & Financial Records *[e.g. Invoices, Receipts, Financial Statements etc.]*	5 years from the end of the financial year in which the	ATO (Income Tax Assessment Act)	Must include sufficient detail to substantiate Tax Claims and GST.

	transaction occurred.		
Company / Corporate Records *[Minutes, Registers, Financial Reports, ASIC filings].*	7 years after the transactions or events are completed.	*Corporations Act 2001* / ASIC	Includes Annual Financial Reports and Director-related documents.
Employee / Payroll Records *[Contracts, Payslips, Rosters, Leave Records, Termination Records, Timesheets, Overtime Records].*	7 years from the date the record was created **or** from the date employment ends (whichever is later).	*Fair Work Act 2009 (s535)* & *Fair Work Regulations*	MUST INCLUDE: • Employee Name; • Start/Stop Times (where required); • Hours Worked; • Overtime Details (Number of Overtime Hours per day OR Start/Stop times of Overtime if Penalty / Loading applies); • Wages Paid; • Deductions; and • Any set-off Calculations. Records must be readily accessible to *Fair Work* inspectors. Applies to both Wages/Salary Employees.
Superannuation Contributions	5 years from the date of the Contribution.	Superannuation Legislation / ATO	Must show contributions made on behalf of each Employee.
Legal / Contractual Documents *[e.g. Agreements, Deeds, etc.]*	7 years after expiry or Termination of the Contract / Agreement.	Limitation of Actions Acts (relevant State/Territory)	Includes Employment Contracts and Service Agreements.
WHS / Incident Records *[Incident Reports, Risk Assessments, Training Records].*	7 years [generally] 30 years for Hazardous Chemicals & Health Monitoring Records. 40–100+ years or Permanent for Asbestos-related Records and Serious / Notifiable Incidents.	Model WHS Laws + Work Health & *Safety Regulation (Qld)* / *Workplace Health & Safety Queensland*.	Longer Periods apply for high-risk incidents (e.g. Asbestos). All Notifiable Incidents must be documented thoroughly.
Workers' Compensation Claims	Duration of the Claim + 7 years	*Workers' Compensation and Rehabilitation Act 2003 (Qld)* and equivalents.	Includes all Claim Documentation, Medical Reports and Related Correspondence.
	7–10 years		

Health / Medical Records (if applicable to Business)	*[or longer depending on State requirements and Nature of the Record].*	State Health Records Acts	Retention may extend significantly for Children or certain Medical Conditions.
NDIS Individual & Service Delivery Records (If applicable to Business) *[Support Plans, Service Agreements, Support Delivery Logs, Rosters, Incident Reports, Evidence of Supports provided, Quotes, Invoices related to Supports].*	7 years after the last Support was provided to the individual *[or longer if required].*	NDIS Act 2013, NDIS Practice Standards, NDIS (Incident Management and Reportable Incidents) Rules	MUST INCLUDE: • Individual Name & Reference Number; • Date(s); • Quantity & Type of Support Delivered; • Location; • Staff involved; • Outcomes Achieved; and • Evidence that supports and aligns with the Individual's Plan. Records are critical for payment Validation, Audits and Compliance with the NDIS Commission. Rosters and Delivery Logs are key evidence.

Important Overarching Rules:

- ***Longer Retention applies automatically*** *in the following circumstances* (normal disposal must be suspended):
    - Any internal or external Audits (including *NDIS Practice Audits* or *ATO* Reviews);
    - Disputes or Complaints (including Employment Underpayment Claims, Complaints or *Fair Work* matters);
    - Legal Holds or anticipated/ongoing Litigation; and/or
    - *NDIS Commission* Requirements or Investigations.

  In these cases, Records must be kept for the duration of the matter plus any applicable limitation period.
- The **Delegated Business Leader** (for Document Control) is responsible for assessing and advising **case-by-case** extended retention periods. All Staff must immediately notify the **Delegated Business Leader** (for Document Control) when any trigger occurs and must not dispose of any potentially relevant records without their written approval.
- Records must be stored securely (with appropriate Access Controls, Backup and Disaster Recovery) and produced promptly if requested by a Regulator, Inspector, Court or the *NDIS Commission*.
- **A Routine Disposal Review and Destruction Activity will occur annually in December**, subject to any extended retention triggers (Audits, Disputes, Legal Holds or *NDIS Commission* requirements).

6. Storage and Management

- **Paper Records**: Store in locked, secure cabinets with restricted access. Protect from fire, flood and unauthorised viewing.
- **Electronic Records**: Use encrypted storage (at rest and in transit), secure Cloud Platforms, Multi-Factor Authentication (MFA), role-based access and Audit Logs. Follow the 3-2-1 Backup rule.
- **Third-Party Providers**: Contracts must include Privacy and Security Clauses aligned with the APPs and *NDIS* requirements *(where applicable)*.

All electronic documents (including emails) follow the same retention and security rules.

7. Information Security Controls (aligned with *APP 11* and *ACSC Essential Eight*)

Password and Authentication Requirements

- Administrator-set passwords must be uniquely and randomly generated via any information system, then immediately changed by the user.
- Use at least 8 characters (upper/lower case, numbers, symbols).
- DO NOT write down or share passwords unless approved. *Always change immediately if compromise is suspected.*
- Use Password Management Tools and enable MFA wherever possible.

Email Security

- Do **NOT** open unexplained attachments or links;
- Always check Sender details for inconsistencies;
- Block any spam / scam;
- Verify Financial or Login Requests by Phone; and
- Contact the **Delegated Business Leader** (for Privacy/Security) if unsure.

Device Security and Personal Devices

- Personal devices for work access are **NOT** recommended.
- Follow Best Practices:
    - Strong passwords;
    - Safe networks;
    - Regular updates and antivirus;
    - Never leave devices unattended;
    - Lock computers when leaving the desk;
    - Segregate your Internet of Things (IoT) (i.e. smart) devices onto a separate network; and
    - Dispose of devices securely.

Transferring Data and Working Remotely

- Avoid unnecessary transfer of Personal or Confidential information;
- Share data ONLY over authorised secure networks and in compliance with the *Australian Privacy Principles* and *NDIS* requirements (where applicable);
- **All rules also apply when working remotely;**
- Use systems for Business purposes only;
- Protect Confidential information; and
- Do not bypass security or install unauthorised software.

General Security Requirements

- Stay up-to-date with recommendations;
- Perform regular Backups;
- DO NOT circumvent controls; and
- ***Report any incidents immediately***.

8. Incident Notification and Reporting Process

All individuals MUST report **any** suspected Security Incident, Privacy Breach, Suspicious Activity, WHS Incident or potential Risk **immediately** *(and within 1 hour where possible)*.

How to Report:

1. Contact the **Delegated Business Leader** (for Privacy/Security) by phone, email or Designated Reporting Channel.
2. Provide Details: What happened, when, what information/systems/records were involved and any evidence.
3. Do **NOT** attempt to investigate or fix the issue yourself unless instructed.

The Business will acknowledge the report, initiate containment/assessment, determine if it is an eligible Data Breach or *Reportable NDIS Incident*, coordinate notifications (OAIC, *NDIS* Commission, WorkSafe etc.) and document lessons learned.

***NDIS*-specific Note *(Only if applicable to Business)*:** Registered Providers must also follow the *NDIS (Incident Management and Reportable Incidents) Rules 2018*, including timely reporting to the *NDIS Quality and Safeguards Commission* for Reportable Incidents. Failure to report promptly may itself be a Breach of this Policy.

9. Document Destruction and De-identification

Records must be retained only as long as they serve a legitimate Business, Legal or Regulatory purpose. Routine Destruction of records that have reached the end of their retention period and are no longer needed will be **Scheduled Annually in December**. This timing allows sufficient opportunity for End of Financial Year adjustments, changes, final reviews, Audits, Legal Holds or other triggers before disposal.

Destruction Methods *(Applies On and Off-site)*

- **Paper Records**: *MUST be destroyed using cross-cut or micro-cut shredding* OR a certified **National Association for Information Destruction (NAID) AAA** service and a Certificate of Destruction must be obtained and retained for each Batch.
- **Electronic Records**: MUST be permanently deleted using secure deletion methods that prevent recovery (e.g. file shredding software or secure erase tools). All copies, including backups, must be removed where practicable.

Identification of Electronic Records for Destruction

To enable efficient identification and destruction of electronic records:

- When creating an electronic record which will in the future require Destruction, staff should ***Append a Destruction Marker to the Filename i.e. ClientFile_D2027*** *(indicating the file is due for Destruction in December 2027)*.
- ***At the end of each year (in December), the Delegated Business Leader will search for files containing the _D20xx Marker (or equivalent) and co-ordinate secure Destruction*** after confirming that no Audits, Disputes, Legal Holds or *NDIS Commission* requirements apply.
- *This naming convention supplements proper folder structures and any Electronic Document and Records Management System (if used)*.

Approval and Records

Destruction may only occur with the written approval of the ***Delegated Business Leader*** *responsible for file Destruction.* A record of all Destructions (including date, description of records destroyed, method used and Certificate of Destruction where applicable) must be maintained for at least 7 years. Personal and Confidential information must be destroyed or de-identified using reasonable measures in accordance with *APP 11.2* and *NDIS Practice Standards*, unless law requires otherwise.

10. Suspension of Document Destruction (Legal Holds)

If there is any indication of an investigation, actual or imminent Legal action, WHS incident, Workers' Compensation Claim or *NDIS* matter, **immediately suspend** all Destruction. The

Delegated Business Leader (for Document Control) will identify and segregate relevant documents. Destruction of segregated items resumes ONLY after the matter concludes.

11. Data Breach Detection and Response

If a Breach is discovered, notify the *Office of the Australian Information Commissioner (OAIC)* using the **OAIC Eligible Data Breach Form** then follow the **OAIC's Four-Step Process**:

1. Contain → Assess → Notify → Review.
2. Log ALL Incidents.

For eligible Data Breaches, notify the OAIC and affected individuals using the **Letter Template in Appendix A**. *NDIS* Providers **MUST** also notify the *NDIS Commission* if applicable.

NEVER Destroy Records related to a KNOWN or SUSPECTED BREACH.

12. Training and Awareness

All individuals within the scope of this Policy receive Induction Training and Annual Refreshers on this Policy, including WHS Record-Keeping, Privacy, *NDIS* obligations (where applicable) and Incident Reporting.

13. Compliance and Disciplinary Action

Breaches (including Failure to Report Incidents) are assessed case-by-case. Intentional, repeated or harmful breaches may result in Formal Warnings or Termination. Immediately notify the **Delegated Business Leader** (for Document Control) of any suspected non-compliance. For queries regarding this Policy, contact the **Delegated Business Leader**.

Appendix A: Template – Notification of Data Breach to Affected Individuals

[Your Business Logo]

[Date]

Private and Confidential
[Full Name of Affected Individual]
[Address]
[SUBURB] [STATE] [POSTCODE]

Dear **[Full Name]**

RE: Notification of an *Eligible Data Breach* Involving Your Personal Information

We are writing to notify you of an *Eligible Data Breach* that has affected some of your Personal Information held by our Business (**[Full Legal Name]** - ABN: **[ABN]**).

We take our Privacy obligations very seriously and apologise for any concern this may cause you.

What Happened?
[Provide a clear description of the breach, including when it occurred or when you became aware of it and how it happened – e.g. "On [date], we discovered Unauthorised Access to our Client Management System due to a Cyber Security incident."]

What Personal Information was Involved?
The kinds of Personal Information involved include your:

- **Full Name;**
- **Date of Birth;**
- **Contact Details;**
- **Details of Supports Provided;**
- **Payment information; and**
- ***NDIS* Reference Number.**

What Have We Done?
We have taken the following Steps to respond to and contain the breach:

- **Secured the System;**
- **Changed Access Credentials;**
- **Conducted a Forensic Investigation;**
- **Notified Relevant Regulators (including the *NDIS* Commission if applicable); and**
- **Enhanced Security Controls.**

We have assessed this as an *Eligible* Data Breach under the *Notifiable Data Breaches Scheme* and have notified the *Office of the Australian Information Commissioner (OAIC)*.

What Should You Do?
To help protect yourself, we recommend you:

- **Monitor your bank accounts and Online Portals for any suspicious activity.**
- **Be wary of unsolicited communications (phone, email or text) asking for your personal details.**
- **Change passwords for any online accounts where you may have used similar login information.**
- **Contact the *NDIS Commission* on 1800 035 544 (if applicable).**
- **[Add any other specific recommendations relevant to the Breach].**

Questions?
Further guidance on responding to a Data Breach or your own rights is available on the *OAIC* website: https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches**.** Otherwise, please contact us via the phone number or email address provided below.

We will contact you again if there are any significant updates. Thank you for your understanding as we work to resolve this matter and strengthen our Protections.

Respectfully

[Full Name]
[Position], [Business Name]

Contact Phone: [Phone]
Contact Email: [Email]