

Data Retention and Deletion Policy

January 2026

TEMPLATE ONLY





[THIS PAGE IS INTENTIONALLY LEFT BLANK]





Contents

Data Retention and Deletion Policy	1
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
5. Data Retention Schedule	5
6. Data Protection and Privacy	6
7. Roles and Responsibilities.....	6
8. Training and Awareness.....	6
9. Policy Compliance	6
8.1 Compliance Measurement.....	6
8.2 Exceptions	6
8.3 Non-Compliance	6
10. Related Standards, Policies and Processes.....	7
11. Revision History	7





1. Introduction

[Company Name] collects, stores, and processes information to support service delivery, operations, and compliance with legal and contractual obligations. While retaining information is necessary for business and security purposes, retaining data longer than required increases cyber security, privacy, and operational risks.

This policy establishes requirements to ensure that information is retained only for as long as necessary and is securely deleted when no longer required. Effective data retention and deletion support cyber security resilience, reduces the impact of incidents such as ransomware, and aligns with the Australian Cyber Security Centre (ACSC) Essential Eight mitigation strategies.

2. Purpose

This policy defines how the organisation retains and securely deletes information to reduce cyber security risk and support the objectives of the **ACSC Essential Eight** mitigation strategies. Proper data retention and deletion limit the impact of cyber incidents, including malware, ransomware, and unauthorised access.

3. Scope

This policy applies to:

- All information and data processed, stored, or transmitted by the organisation
- All systems, applications, endpoints, servers, and backup environments
- All employees, contractors, and third-party users
- All Data formats, including electronic and physical records.

4. Policy

- 4.1 [Company Name] will retain information only where there is a defined business, legal, regulatory, or security requirement.
- 4.2 Retention periods must be documented and approved by the relevant data owner.
- 4.3 Information must not be retained indefinitely without justification.
- 4.4 Retention decisions must consider cyber security risk, privacy obligations, and incident response requirements.
- 4.5 Security, authentication, and system logs must be retained for a period sufficient to support detection, investigation, and response to cyber security incidents.
- 4.6 Backups must be retained in accordance with business continuity and disaster recovery requirements, while minimising long-term exposure to cyber threats.
- 4.7 Information must be securely deleted when it is no longer required or when approved retention periods expire.
- 4.8 Secure deletion methods must prevent unauthorised access, recovery, or reconstruction of information.
- 4.9 Only authorised personnel and systems may perform data deletion activities.





- 4.10 Personal, confidential, or sensitive information must be handled and deleted in accordance with applicable privacy and data protection legislation.
- 4.11 Information subject to legal, regulatory, or investigative holds must not be deleted until the hold is formally lifted.
- 4.12 All data retention and deletion activities must comply with applicable laws, contractual obligations, and internal policies.
- 4.13 Failure to comply with this policy may increase cyber security risk and expose the organisation to legal and regulatory consequences.

5. Data Retention Schedule

[Company Name] retains information only for as long as required to meet business, legal, operational, and cyber security requirements. Standard retention periods are outlined below. Retention periods may be extended where required by law, contractual obligations, or approved operational needs.

Data Type	Description	Retention Period
Security event logs	System, application, and security monitoring logs	Minimum 180 days
Authentication logs	Login, access, and privilege activity	Minimum 180 days
Endpoint and server logs	Endpoint detection and system activity logs	Minimum 90 days
Email logs	Email flow and security logs	Minimum 90 days
Backup data	System and data backups	30–90 days , depending on system criticality
Customer data	Client records and service-related data	7 years after last engagement
Employee records	Employment and personnel records	7 years after termination
Financial records	Accounting, billing, and tax records	7 years
Contracts and agreements	Client, vendor, and partner contracts	7 years after expiry
Incident response records	Incident logs, reports, and evidence	5 years
Temporary working files	Drafts, exports, and transient data	30 days
Audit records	Audit findings and evidence	5 years





6. Data Protection and Privacy

- 6.1 Personal, confidential, or sensitive information must be retained and deleted in accordance with applicable privacy and data protection legislation.
- 6.2 Where possible, data should be minimised, anonymised, or de-identified.
- 6.3 Users must be aware that some systems, including cloud and backup services, may retain data beyond primary systems.
- 6.4 All data handling must comply with relevant privacy legislation and internal privacy policies.

7. Roles and Responsibilities

- 7.1 Management is responsible for approving this policy and ensuring appropriate oversight.
- 7.2 Data owners are responsible for defining and approving retention requirements for information under their control.
- 7.3 IT and security personnel are responsible for implementing technical controls to support retention and secure deletion.
- 7.4 All employees and affiliates are responsible for complying with this policy and reporting concerns or issues.

8. Training and Awareness

- 8.1 [Company Name] will promote awareness of appropriate data retention and secure deletion practices.
- 8.2 Guidance or training may be provided where appropriate to support compliance with this policy.
- 8.3 Staff are encouraged to raise questions or concerns regarding data retention and deletion with management.

9. Policy Compliance

- 9.1 Compliance Measurement
Compliance with this policy may be verified through reviews, audits, system monitoring, and management oversight.
- 9.2 Exceptions
Any exception to this policy must be approved in advance by management.
- 9.3 Non-Compliance
Any individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or engagement.





10. Related Standards, Policies and Processes

- Privacy Policy
- Information Security Policy
- Incident Response Policy

11. Revision History

None.

