Backup & Retention Policy

Last Modified on 26/10/2026 11:36 am AEDT

Customer Data Backup and Retention

In this guide '**Customer Data**' means information and content owned and controlled by a ReadiNow Customer (including any File repository data) held in the Customer's tenant.

1. Backup

1.1. Backup Frequency

ReadiNow performs regular backups of customer data to support business continuity and disaster recovery. Backup processes are designed to meet the platform's documented recovery objectives:

- Recovery Point Objective (RPO):
  - Database data: 30 minutes
  - File repository data: 24 hours
- Recovery Time Objective (RTO):
  - Database services: 6 hours
  - File repository data: 4 hours

Backup and disaster recovery processes are regularly tested to verify their effectiveness and support reliable restoration of customer data.

1.2. Backup Retention

Backups are retained for at least 90 Days

1.3. Backup Security

All backups are encrypted using industry-standard encryption. Backup data is stored in secure AWS storage and protected through layered security controls, including restricted administrative access and least-privilege access controls. Platform backups are retained in accordance with ReadiNow's backup retention policy and protected against unauthorised access, modification and deletion.

1.4. Data Residency

All customer data, including live and backup data, resides in AWS data centres located in Australia.

2. Restore/Data Recovery

2.1. Recovery Requests

A Customer may request a restoration from a backup by submitting a Support ticket in the ReadiNow Service Desk.

The recovery time depends on the age of the backup and the amount of Customer Data to be recovered. Such requests are chargeable and will be estimated and quoted prior to fulfilling the request.

2.2. Recovery Format

The recovered Customer Data will be in one of the following formats:

- Access to a temporary tenant; or
- CSV files; or
- As otherwise advised via ReadiNow Service Desk, at ReadiNow's sole discretion.

3. Data Destruction

3.1. General

ReadiNow does not delete records from active tenants. Customers should refer to the Log Retention Policies article for information on configuring log archiving frequencies.

All customer data, including backup data, is held within AWS at all times. ReadiNow does not maintain any physical media holding client data. Therefore, destruction of media is performed by AWS.

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned. For further information please refer to the data centre controls published by AWS.

3.1. Customer Disengagement

In the event of customer disengagement, active tenants will be deleted within 30 days. ReadiNow will ensure the security of backups from multi-tenanted systems until the backups can be deleted in line with the backup retention period. Backups from dedicated systems will be deleted within 30 days.