Backup & Retention Policy

Last Modified on 12/03/2024 12:50 pm 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

Full backups are taken daily and transactional log backups are taken every 20 minutes.

Note: Customer Data that is present for less than this time period may not be captured by the backup process and hence may not be recoverable (i.e. Customer Data that is created and subsequently deleted between the backup periods).

1.2. Backup Retention

Backups are retained for at least 90 Days

1.3. Backup Security

All backups are encrypted. Encryption processes and methods follow AWS' data encryption standards in line with ISO 27001 standards across all their infrastructure and hosting environments. The platform backups are protected from accidental or malicious modification or erasure using the Amazon S3 Object Lock technology. No one, including ReadiNow staff, can modify or delete a backup by any means, for a minimum of 90 days.

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.