Backup and Media Handling Policy

Version 9

REZOLVE.ai

Document Information

Name of the document	Backup and Media Handling Policy
Release date	19-Dec-18
Owned by	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	04-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	01-Mar-2023	Reviewed and no change
7	13-Sep-2024	Updated Document Information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	08-May-2026	Reviewed and no change

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder&CTO	Approved	13-May-2026

Table of Contents

Policy Statement

Purpose

The availability of data relating to business applications and essential standing data necessary for the effective operation of the IT infrastructure shall be ensured through the availability of backup copies of such information and applications that are taken regularly and tested periodically to ensure their integrity.

Objective

The objective of this policy is to outline the requirements for effective backup of data and critical applications to ensure systems are restored securely in the event of any disruption such that business is not interrupted. Additionally, to ensure the security of information handled during business operations and held on data storage media is protected against loss, tampering, or disclosure, and to ensure secure handling of information on removable and portable media.

Scope

This policy is applicable to relevant Rezolve.ai Information Services (Rezolve.ai) information assets and all employees of Rezolve.ai, its contractors, and third-party users in employment or in contract with Actionable Science Labs who directly or indirectly cater to Rezolve.ai, as detailed in the Rezolve.ai Information Security Policy.

Approval

This policy bears the approval of the ISMS Steering Committee, and the implementation and operation of the policy shall be the responsibility of the ISMS Steering Committee and the IT Admin Department of Rezolve.ai.

1. Requirements

Backup Process

a. Backup Process
Rezolve.ai shall establish backup processes that define the type of information to be backed up, backup cycles, and methods of performing backups.

b. Information Resources to be Backed Up
Information resources to be backed up shall include:

- Business data
- Business applications
- Data necessary for the proper functioning of devices and equipment
- Control information stored in primary and secondary storage devices of servers
- Network and security devices
- Desktops, laptops, and handheld devices

c. Backup Approval and Compliance
The backup process shall be approved by the business owners and comply with business continuity, legal, and regulatory requirements. All backup and restoration logs shall be maintained for retention periods as defined in the "Backup and Restoration Procedure."

d. Critical Data Backup
Critical data and information, key software applications, network configuration files, critical server configurations, other device configurations, and system documentation shall be backed up as per business and procedural requirements.

e. Automated Solutions
Where feasible, automated solutions shall be used for data backups. These shall be tested prior to implementation and at regular intervals. Company uses cloud provider tools for backups.

f. Protection Measures

Backups shall be protected from loss, tampering, damage, and unauthorized access.

g. Storage of Backup Media
Backup media shall be stored securely, protected from natural and man-made hazards.

h. Offsite Storage
Not applicable – all backup is done on the cloud.

i. Portable Media Backup
Not applicable – company does not use portable media.

j. Periodic Assessment
Cloud storage arrangements shall be assessed annually for security and safety compliance.

k. Backup Testing
All backups shall be tested periodically to ensure successful data restoration without loss.

l. User Training
Users shall receive training on their responsibilities related to data backup.

m. Backup Frequency by Information Type

- **Business Data**: Daily backup for one week
- **Critical Applications**: Source code version control in Bitbucket
- **Control Information (servers, network devices)**: As per cloud standards
- **Desktops and Laptops**: No critical data stored
- **Portable Media**: Not applicable
  (Frequency can be adjusted as per business/regulatory needs.)

2. Media Handling

a. Management Procedures
Rezolve.ai shall define procedures for managing removable media—authorization, usage, inspection, retirement, and disposal.

b. Authorization for External Use
Prior approval is needed for media used outside the organization. All requests shall be tracked via Jira IT Tracker.

c. Safe Storage
Data shall be stored in line with cloud storage standards in secure environments.

d. Removable Media Drives
Allowed only for business needs, and use must be authorized. Misuse for personal reasons is prohibited.

e. Secure Disposal
Media shall be securely disposed of as per criticality of data following the information classification guideline. Disposal is tracked in the IT Tracker project.

f. Inspection Before Disposal
All storage devices shall be inspected by the technology team before disposal and formally signed off.

g. Training for Secure Disposal
Rezolve.ai provides training on secure media disposal.

h. Handling Confidential Information

Procedures shall be in place for handling and storing sensitive information.

i. Access to Documentation
User/system documentation is available on a need-to-know and need-to-do basis only, with appropriate approval. It must be kept current and regularly reviewed.

3. Roles & Responsibilities

Roles	Responsibilities
IT Admin Department	- Policy implementation and monitoring of key parameters
Department Heads & Staff	- Adherence to backup procedures applicable to them
ISMS Steering Committee	- Approval of policy and overall governance
CISO	- Formulation and oversight of policy implementation

4. Compliance

a. Disciplinary Action
Policy violations may lead to disciplinary action under the Code of Conduct, including dismissal or legal action.

b. Investigation
Alleged violations and associated events are subject to investigation.

NOTE: Next review cycle for this policy is March 2027. Management may review or amend the policy earlier based on circumstances.
All references to Actionable Science in this policy are equivalent to Rezolve.ai.