Remote Work Policy

Version 8

REZOLVE.ai

Document Information

Name of the document	Remote Work Policy
Release date	14-July-2020
Owned by	Neil Dattani
Governed by	Mr. Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	12-July-2020	Initially Drafted
2	14-July-2020	Final
3	03-June-2021	Reviewed and change, Prior approval for short leaves, Extended till March.
4	11-Mar-2022	Added applicability, compliance with policies and updated document information
5	03-Mar-2023	Reviewed and no change
6	27-Sep-2024	Reviewed and no change
7	24-Mar-2025	Reviewed and no change
8	07-May-2026	Annual review completed. Minor editorial validations.

Reviewer and Approver

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

Table of Contents

Purpose....2
Applicability....2
Policy....2
Equipment....2
Compliance with Policies....3

Our Employee remote work policy outlines our guidelines for employees who work from a location other than our offices. We want to ensure that both employees and our company will benefit from these arrangements.

Purpose

This policy outlines guidelines for employees to work from a location other than their office premise. Rezolve.ai considers this policy to be a viable, flexible work option when both the employee and the job responsibilities are well-suited for it. This policy does not alter the terms and conditions of employment and is intended to support secure, productive, and compliant remote working arrangements.

Applicability

This policy is applicable to all those employees who are unable to work from office location in following conditions:

- Employee is having some medical emergency/conditions.
- In case of natural disaster and pandemic situation nearby office location or employee location.
- In case of infrastructure issue or any other issue in office location due to which employee is unable to work from office location.
- Due to any other reasons for which employee has taken prior approval from the management.
- Management has granted approval to selected employees based on their locations/working hours.

Prior approvals are needed from the management, except in case of natural disasters, pandemic situations, management themselves have granted approval to employees based on their location/shifts/working hours.

Employees must send an e-mail to either **neil.dattani@rezolve.ai**, **aanchal.saini@rezolve.ai**, **ub@rezolve.ai**, **saurabh@rezolve.ai**, **manish@rezolve.ai** along with their respective team lead/manager - stating reason with supporting attachments (if applicable) along with the duration for remote work (start date and end date).

Policy

To ensure that employee performance will not suffer in remote work arrangements, we advise our remote working employees to:

- Choose a quiet and distraction-free working space.
- Continue to work in regular working hours as usual and ensure their schedules overlap with those of their team members for as long as is necessary to complete their job duties effectively.
- Have an internet connection that's adequate for their job.
- Dedicate their full attention to their job duties during working hours.
- Adhere to break and attendance schedules agreed upon with their manager.
- Have to plan their personal work accordingly, which can be planned 1-2 days in advance e.g. visiting a bank, appointment with the doctor, etc. — so that meetings and other work activities are not disrupted.
- Have to take prior approval for short leave of 1-2 hours from their manager and have to inform HR.
- *Have to inform on **All-rezolve.ai Teams channel** when taking a break.*
- Employees working remotely must ensure that company data is accessed only through approved devices, secure networks, and authorized communication channels in accordance with Rezolve.ai security policies.
- Use of public or unsecured Wi-Fi networks without approved security controls such as VPN is prohibited while accessing company systems or customer data.
- Employees must ensure that confidential or customer information is not disclosed to unauthorized individuals, including family members, roommates, or third parties while working remotely.

Equipment

Equipment that we provide is company property. Employees must keep it safe and avoid any misuse. Specifically, employees must:

- Keep their equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Install only company-approved or authorized software and refrain from downloading unauthorized, malicious, or unlicensed applications.

Company-issued devices may be subject to security monitoring, endpoint protection, logging, and remote management controls to safeguard company and customer information assets.

Compliance with Policies

Our remote employees must follow our company's policies like their office-based colleagues. Examples of policies that all employees should abide by are:

- *Employee NDA*
- *Employee Code of Conduct*
- *ISMS*
- *Acceptable Use Policy*
- *Clear Desk and Clean Screen Policy*
- *Access Control Policy*
- *Backup and Media Handling Policy*
- *Infrastructure Hardening Policy*
- *Password Administration Policy*
- *Privacy Policy*
- *Leave Policy*

NOTE – Next review cycle for this policy is **March-2027**. Management reserves the right to review and update this policy periodically based on business, regulatory, security, or operational requirements.

All documents related to policies and procedures and reference to Actionable Science is as good as Rezolve.ai