Acceptable Use Policy

Version 9

REZOLVE.ai

Document Information

Name of the document	Acceptable Use Policy
Release date	19-Dec-18
Owned by	Mayank Baghel
Governedby	Mr.Udaya Bhaskar Reddy

Revision History

VersionNo	Version Date	Details of Change
1	13Nov-2018	Initially Drafted
2	10Dec-2018	Final
3	15Dec-2020	Reviewed and no change
4	01Dec-2021	Reviewed and no change
5	04Mar-2022	Updated Document Information
6	07Mar-2023	Reviewed and no change
7	12-July-2024	Updated document information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and no change

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Table of Content

Purpose

Overview and Purpose

Chief Information Security Officer's CISO has established this Acceptable Use Policy to protect Rezolve.ai. employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.
Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Rezolve.ai. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.
Effective security is a team effort involving the participation and support of every Rezolve.ai. employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
The purpose of this policy is to outline the acceptable use of computer equipment at Rezolve.ai. These rules are in place to protect the employee and Rezolve.ai. Inappropriate use exposes Rezolve.ai to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope
This policy applies to:

- All electronic and computing devices owned or leased by Rezolve.ai.
- All employees, contractors, consultants, temporary and other workers at Rezolve.ai.
- All operations areas, IT systems, data, and network resources within Rezolve.ai.
- All users accessing Rezolve.ai. systems, whether onsite or remotely

General use and Ownership

- All proprietary information stored on electronic and computing devices remains the sole property of Rezolve.ai. Users must ensure that this information is protected according to the Data Protection Standard.
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Rezolve.ai. proprietary information.
- Users may access, use or share Rezolve.ai. proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet / Intranet / Extranet systems. In the absence of such policies, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Rezolve.ai may monitor equipment, systems and network traffic at any time.
- Rezolve.ai reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Remote Working Policy.
- System level and user level passwords must comply with the Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from Rezolve.ai email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly my own and not necessarily those of Rezolve.ai., unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of Rezolve.ai authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Rezolve.ai-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Rezolve.ai
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Rezolve.ai or the end user does not have an active license is strictly prohibited.
- Accessing data, servers, or accounts without explicit authorization, even if you have access rights, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using Rezolve.ai computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Rezolve.ai account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to CISO is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Rezolve.ai network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program / script / command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet.
- Providing information about, or lists of, Rezolve.ai Employees to parties, except for in due course of work, outside Rezolve.ai.

Email and Communication Activities

- When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information including impersonating another user or entity.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Rezolve.ai networks of other Internet / Intranet / Extranet service providers on behalf of, or to advertise, any service hosted by Rezolve.ai. or connected via Rezolve.ai. network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

- Blogging by employees, whether using Rezolve.ai property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Rezolve.ai systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Rezolve.ai policy, is not detrimental to Rezolve.ai best interests and

does not interfere with an employee's regular work duties. Blogging from Rezolve.ai systems are also subject to monitoring.

- Rezolve.ai Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Rezolve.ai confidential or proprietary information, trade secrets or any other material covered by Rezolve.ai. Confidential Information policy when blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Rezolve.ai and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Rezolve.ai. Non-Discrimination and Anti-Harassment policy.
- Employees may also not attribute personal statements, opinions or beliefs to Rezolve.ai. when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Rezolve.ai. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Rezolve.ai trademarks, logos and any other Rezolve.ai intellectual property may also not be used in connection with any blogging activity

Compliance
The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and direct feedback.

Non-Compliance
Employees found to have violated this policy will be subject to disciplinary action, which may include verbal or written warnings, suspension, and up to termination of employment, depending on the severity of the violation.

NOTE - Next review cycle for this policy is March-2027. Management can review policy any time and can make changes depending on the situation.
***** All documents related to policies and procedures any reference to Actionable Science is as good as Rezolve.ai