Access Control Policy

Version 9

Document Information

Name of the document	Access Control Policy
Release date	19-Dec-18
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

RevisionHistory

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	01-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	07-Mar-2023	Reviewed and no change
7	13-Sep-2024	Reviewed and no change
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and updated

Reviewer and Approver

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

Table of Content

Purpose

Purpose

To control Physical and logical access to information, information systems and information processing facilities maintaining business and security requirements to ensure information confidentiality, integrity and availability.

Principles

- All access to production systems will be granted only against approved Access From. Read access will be approved by the team lead while any privileged access (that allows to make changes to the production system) will be approved by the CEO / CISO.
- All production assets are assigned owners who are responsible for defining access rights and for evaluating access based on job roles.
- Account sharing is prohibited unless a written approval is granted by the CEO/CISO.
- The asset owners periodically review access to their assets.
- All production systems not using the shared sign-on functionality are required to be implemented with separate user ID and password submission.
- External access to production system by employees is permitted only throughan VPN.
- Privileged access to production resources is restricted to defined user roles and access to these roles must be approved by the CEO /CISO. This access is reviewed by the designated information security officer on a periodic basis as established by the CEO /CISO.
- Access is removed for exiting employees on the last day.
- Logical access controls and change management tools restrict the ability to migrate between development, test, and production to change deployment personnel.
- Access to Gambling,Games,Pornography,URL translations,Extremist websites are blocked.
- Exitemployee deactivated accounts reactivation is done only if approved via CEO/CISO.
- Access to Shared, Generic and accessing accounts of exited employee can be granted only on approval of CEO / CISO.
- Access to Printers given to the users based on the roles and as per special permissions approved by the CEO/ CISO.

Policy Statement/Control

- Implement access control procedures to control access to security assets in accordance theAccess Control Procedure.
- Users should be authenticated using unique ID and password for access to all Rezolve.ai systems.
- Access to the system with shared Sign-on is not allowed as a policy, access to the system to be given only by using Separate User ID and Password.
- User access including privileged IDs shall be restricted based on a need to know basis and should be set to "DENY ALL" unless specifically allowed.
- Segregation of duties shall be implemented.
- All access shall be approved electronically or in writing by authorized parties and reviewed every yearly for continued validity.

- Implement Password Policy across the Organization.
- To communicate need for information and information system access control.

Scope

- This policy covers logical and physical boundaries of Rezolve.ai.
- This policy covers all Rezolve.ai network, Operations area, IT systems, data and authorized users, Public users within logical and physical boundaries.

Access Process

Access request /modification/deletion process

- This section is for access request for the following resources
- Code repository
- Cloud/On-premise Development, staging & Production environment.
- Hosted servers
- Website code & contents
- System security is based on public key/private key SSH based infrastructure and / or Password protected. Desktops and laptops require passwords as per Password Policy that must be changed every 60 days, privileged user passwords should be changed every 60 days.
- Employees connecting to Rezolve.ai servers hosted at a 3rd party data center have to login via SSH Password base authentication to ensure that only valid users gain access to Company's data centers.

Access request/modification

- IT Tracker Jira project used for creating all access requests and would be implemented as per the workflow defined.
- Employee access to protected resources is created or modified by the Infrastructure team based on an authorized change request. All higher-level access has to be approved by the CTO.
- Only DEV-OPS engineers have admin access to servers.
- For privileged access CISO's approval will be required on the request form.
- Where Rezolve.ai team have access to the customer server's / website / database as a managed service, access control managed by Rezolve.ai as per the instructions emailed by the Customer.

Access Deletion

- Once resignation is accepted HR will send an Exit Form and / or email notification informing ITteam about the exit and the date when employee will leave.
- As part of no dues process exiting employee's access will be communicated toTeam Lead and same will be revoked. Employee user ID will be removed from each resource and will email id will remain suspended.

Password Policy

General

- All system-level passwords (including root, enable, Windows Administrator, application administration accounts) must be changed in sixty days.
- All user-level passwords (including email, web, desktop computer, laptops, Network devices) must be changed in sixty days.
- Awarning should be generated on logging in10days prior to the expiry of the password.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Alluser-levelandsystem-levelpasswordsmustconformtotheguidelinesdescribedbelow.
- All servers, desktop and laptop computers account Lockout Policy shall be set to an account lockout duration of 30 minutes. The account lockout threshold should be 5 invalid logon attempts. The account lockout counter shall be reset after 30 minutes.

Guidelines

General Password Construction Guidelines

- All users at Rezolve.ai should be aware of how to select strong passwords.
- Microsoft managed password settings is used for accessing all Office 365 and Azure related access.
- Other applications: Strong passwords have the following characteristics:
- Contain at least three of the five following character classes:
    - Lowercase characters
    - Uppercase characters
    - Numbers
    - Punctuation
    - "Special" characters (e.g. @#$%^&*()_+|~-=`{}[]:";'<>/ etc)

- Contain at least eight alphanumeric characters.

- Weak passwords have the following characteristics:
    - The password contains less than eight characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
        - The words "Rezolve.ai", "Gurgaon", "London" or any derivation.
        - Birthdays and other personal information such as addresses and phone numbers.
        - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards.
        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Password Protection Standards

- Always use different passwords for different accounts from other access.
- Always use different passwords for various access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored online without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications.
- If an account or password compromise is suspected, report the incident to the CISO.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Application security restricts output to approved roles or user IDs.
- Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.
- Application-level security restricts the ability to access, modify, and delete data to authenticated users who have been granted access through a record in the access control list. Creation and modification of access control records occurs through the access provisioning process.

Remote Access Users

- Access to the Rezolve.ai Networks and customer VPN via remote access is to be controlled using group policy defined based on roles.
- It enables creation of point-to-point encrypted tunnels between the remote user and the company's internal network, requiring a combination of SSL certificates and a username/password for authentication.
- Privileged customer accounts are created based on a written authorization request from the designated customer point of contact. These accounts are used by customers to create customer user access.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Cloud Authentication

- SSH with public-key cryptography is used to authenticate with remote systems.
- Private key is stored on the laptop and is in the custody of the user.
- Two-factor authentication will be mandatorily used with the private key.
- Remote root login is disabled on production servers.
- Only selected members from the Infra team have administrative access to all servers.
- If a private key is lost or compromised, the user will generate another public/private key pair and will send the public key to the infrastructure team through an email, which will be retained by the IT team.
- Internal VPN connection encryption is AES-128 and the authentication algorithm is MD5.
- For internet access, the connection to the portal is HTTPS-enabled (SSL).
- Employees accessing SAAS services and working from home / not accessing from office premises are not authenticated.
- Employees accessing customer's network via customer VPN and working from home / not accessing from office premises are not authenticated.
- Switches have been configured by ISPs in a way that IPs cannot be cloned.
- The online application matches each user ID to a single customer account number. Requests for access to system records require the matching of the customer account number.
- External access to the nonpublic area of the website (for login to client areas) is restricted through the use of user authentication based on HTTPS and encrypted through secure TLS.

System / Cloud Administrator Access

- Admin access to the cloud system is with DEV-OPS engineers.
- On-premise admin access is with IT Senior Executive.

Access Audit

- Once every quarter, the CISO will review access and compare it to the HR list for any leavers still having access.
- He will take a sample of new employees and leavers and verify that their access addition/deletion requests have been properly approved and filed.
- Once every quarter, access lists for each team’s resources will be sent to the Team Lead, who will review them against approved forms. Any exception will be corrected immediately. Access audit review will be discussed in review meetings.

Records

- All approvals and access rights will be tracked in the Jira tracker.

NOTE – The next review cycle for this policy is March 2027. Management can review the policy at any time and make changes depending on the situation.

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