Physical and Environmental Control Policy

Version 7

REZOLVE.ai

Document Information

Name of the document	Physical and Environmental Control Policy
Release date	15-Dec-2021
Owned by	Aanchal Saini
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Dec-2021	Initially Drafted
2	15-Dec-2021	Final
3	04-Mar-2022	Updated Document Information
4	03-Mar-2023	Reviewed and no change
5	26-Sep-2024	Reviewed and no change
6	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
7	12-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

Purpose and Scope

Purpose
This policy talks about physical and environmental aspect of security that includes how physical access should be provided to employees as well as visitors, environmental security, inspection of incoming and outgoing packets etc.

Scope
This policy applies to all employees, vendors, Employees of Third Parties, Consultants accessing the resources of Rezolve.ai. Resources include any type of resources that belongs to Rezolve.ai or available in Rezolve.ai premises. However, it does not include Storage, Backup Media Protection and Disposal of Assets.

IT team shall segregate the physical layout of processing facilities into perimeter zones. Each zone will have a higher level of access restrictions and access authorization requirements. The perimeter zones are:

- **Public Zone and/or Reception Zone** (Limited restrictions - area under overall surveillance)
- **Office Zone** (Limited access - access permission required. Area under overall surveillance)

Accountability

CEO / CTO shall ensure that all Physical security controls are deployed across all locations and end users are trained on their usage.

Policy Standards

Physical Access Security

General Standards

- All staff and visitors shall wear some form of visible identification.
- All Rezolve.ai employees are prohibited from sharing ID cards to access Rezolve.ai premises.
- Supporting services contractor's personnel shall be granted restricted access to secure areas zone only when required and it shall be monitored.

Physical Access Control for Areas Containing Sensitive Information

- Access to every office and work area containing sensitive information must be physically restricted to those with a need-to-know.
- When not in use, sensitive information must always be protected from unauthorized disclosure.
- When left in an unattended room, information in paper form must be locked away in appropriate containers (safes, file cabinets, etc.).

- During non-working hours, employees in areas containing sensitive information must lock-up all information.

Multi-user Computer or Communication Systems

- All multi-user computer and communication equipment must be located in monitored areas to prevent tampering and unauthorized usage.
- All switches, hubs, routers and other network equipment must be locked or must be placed at a place where it can be continuously monitored.

Guards for Areas Containing Sensitive Information

- Guards for areas containing sensitive information shall be deployed as needed and must be trained to monitor and report any unauthorized access or suspicious activities.

Visitor or Third-Party Access

- Visitor or other third-party access to company offices, computer facilities, or other work areas containing sensitive information must be controlled by guards maintained by building administration or other designated staff.

Reporting Lost/Stolen Identification Badges

- Identification badges that have been lost or stolen, or are suspected of being lost or stolen, must be reported to the HR department immediately.
- The admin must take steps to immediately block the privileges associated with these badges (if any).

Piggybacking or Tailgating Prohibited

- Each person must wear his or her ID card before entering any controlled door within company premises.
- Employees must not permit unknown or unauthorized persons to pass through doors, gates, or other entrances to restricted areas simultaneously with them.

Propped Open Doors to Sensitive Areas

- Whenever doors to sensitive areas are propped open (e.g., for moving computer equipment, furniture, supplies), the entrance must be continuously monitored by an employee.

Testing Physical Access Controls is Forbidden

- Employees must not attempt to enter restricted areas in company buildings for which they have not received access authorization.
- If employees need access to a certain area, they must go through the proper authorization channels.

Physical Security for All Computer Media

- All information storage media (such as HDDs, SSDs, USBs) containing sensitive information must be physically secured when not in use.
- The intention of this guideline is to ensure that all managers implement physical security measures for sensitive information.

Building Access Control System Records

- The Security Department (owned by building administration) maintains records of persons currently inside company buildings to facilitate emergency evacuation and support investigations.
- This information is securely retained for at least one month.

Physical Access Control and Rights Changeover After Employee Separation

- When an employee terminates his or her working relationship with the company, all physical security access codes known by the employee must be deactivated or changed.
- All access rights to company restricted areas must be immediately revoked upon employee termination.

Physical Access Control System

- Facilities and Administration should position access control devices at main entry points.
- CCTV cameras should be deployed in critical areas, and all movements should be monitored and recorded.
- CCTV footage should be retained for a minimum of 30 days before recycling.
- The access control system should record all employee entry and exit events.
- A monthly report on access data should be reviewed. Any suspicious entry should be investigated and reported to the appropriate authority.
- Reports should be maintained for a period of 30 days.

Handling Visitors

Sign-In Process for All Visitors

- All visitors must sign in at the main gate and other sensitive area gates prior to gaining access to restricted areas controlled by the Company.
- Visitors must be admitted to Company premises only for specific authorized purposes.
- Visitors shall be provided with a visitor pass as soon as they enter their details in the visitor register.

Escorted Visitors

- Visitors to Company offices must be escorted at all times by an authorized employee.
- This means that an escort is required as soon as a visitor enters a controlled area, and until the visitor exits the controlled area.

Third-Party Supervision in Areas Containing Sensitive Information

- Individuals who are neither Company employees, authorized contractors, nor authorized consultants must be supervised whenever they are in restricted areas containing sensitive information.

Individuals Without Identification Badges

- Individuals without a proper Company identification badge in a clearly visible place must be immediately questioned about their badge.
- If they cannot promptly produce a valid badge, they must be escorted to the security desk.

Request for Providing / Revoking Access

New Access Request

Employees

- Whenever a new employee joins, HR in coordination with the Administrator shall identify the required areas of access and configure the access control system, including biometric access.
- Similarly, when an employee leaves, HR and the Administrator shall ensure the access is deactivated.
- Employees must use biometric access to enter the office.
- Loss of a Company ID card must be reported to the Admin and HR team. A replacement card will be issued.

Non-Employees

- Individuals involved in housekeeping, security maintenance, electrical maintenance, etc., fall under this category.
- This group of non-employees may have access to all zones but must be escorted when inside critical areas.
- All client representatives will be identified through their visitor tags and will only have access to specific, authorized areas.

Revoking Access Request

- When an employee leaves the organization, the HR/Admin team must complete the employee exit checklist clearance.
- The Admin makes an entry in the access control register by recording the deactivation date.
- The Admin will verify deactivation details monthly by reviewing the entries in the access control register.
- Additionally, when an employee resigns, the employee's Manager must send an email to the Admin department stating the employee's last working day.
- An appropriate entry will then be made in the access control register to reflect access revocation on the employee's final working day.

ID Card Usage Guidelines

The following guidelines must be strictly adhered to regarding ID card usage:

- The identity card must be worn and clearly displayed at all times during office hours and presented for verification when requested by the security officer.
- Always use your own ID card for entry into the premises.
- Lending your ID card, assisting others to gain entry (tailgating), or tampering with access control systems (e.g., biometric devices) is a serious violation. Such actions will result in immediate deactivation of access rights and confiscation of the ID card.
- Ensure that doors equipped with access control remain firmly closed when not in use.
- Do not leave your ID card unattended or misplaced at the workplace, as it may get damaged or lost.
- Never lend or borrow an ID card.
- Keep your ID card safe from physical damage, theft, or loss.
- If your ID card is lost, report it immediately to the HR/Admin department.
- If you encounter anyone not wearing an ID card or visitor pass and you do not recognize them, politely challenge them. This helps identify unauthorized individuals on the premises.
- Report any observed security breaches immediately to the HR/Admin department.
- In cases where biometric or auto-door systems are non-functional, access may be granted by manually opening access-controlled doors.
- Biometrics are integrated with the Attendance Software. The first and last punches of the day are considered for attendance calculation.
- The ID card must be surrendered to the Admin department during the employee exit process as part of the relieving formalities.

Without ID Card Usage Guidelines

If an employee forgets their ID card:

- A temporary ID card will be issued by the Admin.
- Requests for a new ID card must be accompanied by authorization from the respective team lead.

Restriction on Movement of Materials

1. All incoming and outgoing materials must be approved by HR/Admin.
    - A gate pass, duly authorized by the appropriate authority, must accompany any material being moved in or out of Rezolve.ai premises.
2. **Work Area Security**
    - Access to work areas must be restricted to authorized personnel only.
    - Vendors and third-party representatives visiting work areas must be escorted at all times.

- Offices must be equipped with fire detection and prevention systems.
- Standard fire extinguishers must be available and maintained for use in case of fire emergencies.

Other Physical Security Measures

Physical Access Audits

- The Administration team shall **review the list of individuals with physical access to sensitive areas on a quarterly basis** to confirm continued business necessity.
- Admin will also **monitor the visitor log maintained by building security** to ensure compliance with access protocols.

Precautionary Controls

- **Use of device cameras** inside company premises is discouraged to protect sensitive information.
- Employees are advised **not to bring or use mass storage devices** such as pen drives, iPods, or other high-capacity portable storage media.
  - **Rezolve.ai is not responsible** for the safety or security of such devices if they are deposited or left at the security checkpoint.
  - Employees should **avoid carrying any devices capable of data storage** without prior authorization. Violations will be strictly addressed.
- All **visitors' and vendors' baggage must be checked** for electronic devices capable of storing data.
  - Building security may **record these devices** in the visitor register upon entry.
  - Upon exit, **materials will be cross-verified** against the initially declared items to prevent unauthorized data removal.

Emergency and Lighting Measures

- A list of **emergency phone numbers must be maintained** and kept **readily accessible** at key locations.
- **All office areas must be adequately lit** to support visibility and enhance physical security.

Manned Security

Security Guard

There is a building-maintained **Guard 24 hours on working days** at the building entrance. Additionally, **CCTV cameras monitoring** is available on the premises and at the office entrance.

Environmental Controls

Protecting Against External and Environmental Threats

- The **IT team**, in coordination with other departments, shall ensure that **environmental controls are designed and applied** to minimize damage resulting from fire, flood, earthquake, explosion, civil unrest, and other natural or human-caused disasters.
- The design of environmental controls shall:
  - **Comply with health and safety regulations and standards**.
  - **Consider security threats** from neighboring premises.

The IT team shall ensure that:

- **The information processing facilities are not located in an environmentally unstable area.**
- **The information processing facilities are not located near any dangerous neighboring facilities (e.g., chemical laboratories, etc.).**
- **The installed fire detection and fighting equipment meet the requirements defined by the manufacturers.**
- **Full backup equipment and backup media are stored at a safe distance from the main site** to avoid exposure to the same disaster affecting the main site.

Fire Damage

- Proper **fire prevention and detection mechanisms** should be in place.
- A **First Aid Box is available** with security.

Reacting to fire contingencies:

- As soon as a fire breaks out, the **fire alarm should be activated automatically**.
- **Inform the Incident Response Team (IRT) immediately.**

Safety Measures Within the Restricted Areas

- **Smoking is prohibited** in Rezolve.ai premises except in identified areas.
- **Inflammable material such as paper should be stored away** from the work area, and computer printouts within the work areas should be restricted to a minimum.
- **Fire extinguishers and fire exits should be marked clearly.**
- **Fire Exit display boards should be hung at visible places** on each floor, with fire exit routes clearly marked in **red** (preferably fluorescent color), **green**, and **white**.
- The **Admin/IT should arrange for periodic inspection of the fire protection system.**
- **Proper training should be given to all staff members** on the use of safety measures.

Water Damage

- **The hardware could be covered when not in use.**
- **Water and other liquids should not be allowed in the sensitive areas**, as machines and cables could get damaged if there is spillage.

Electrical Damage

- **Qualified electrical personnel should be available** to attend to any repair services.
- **The electrical panels should be a restricted area** and should be **monitored for unwanted movements.**

Evacuation Plan

The evacuation activities for **Rezolve.ai** offices are listed below.

- Employees will inform **Security desk** or inform **Administration** about any hazard conditions possibly leading to a disaster situation or about an actual disaster situation.
- When notified to evacuate, all employees and non-employees will do so in a **calm and orderly fashion** from stairs unless instructed otherwise.
  Here are some guidelines:

    - **walk, don't run;**
    - **keep conversation to a minimum;**
    - **do not take your valuables;** and
    - **go to the designated assembly area** or as instructed during the disaster declaration notification if designated assembly area is not available.
- **Security will keep door open.** They will also remove any doormats or any other obstruction that can impede evacuation.
- If safety permits, Security will not allow any of company's assets such as **laptop computers** to be moved out of the premises.
- In any case, **Security will work with Police and Fire Services** to secure the premises against any looters etc.
- **Administration will contact property manager** to alert them of the disaster situation and the ongoing evacuation.
- If necessary, evacuation will have to be coordinated with other floors.
- If time permits, **Administration will shut down electrical and other systems on the floors** to prevent any adverse effect on the disaster situation or any damage.
- **Designated HR team member will collect the attendance for subsequent roll call.**

Evacuation of Training Participants or Visitors

When an evacuation alarm is sounded:

- Any person in charge of a **training class, seminar or other meeting** should instruct training participants and visitors to proceed **quietly and quickly to the nearest exit**.
- When all employees and visitors have left the room, **the person in charge should leave and close the door** to prevent spread of fire and smoke.

Evacuation of Disabled Persons

- Any disabled person should be assisted by **other employees or by Security** to safely descend to assembly point.
- This should not be done until other people have been evacuated so as **not to impede a smooth evacuation**.

Other Environmental Measures

Power Supply

- **Power going to computer systems should be through uninterruptible power system (UPS).**
- It should be ensured that the **UPS is always in working condition**.
- **Circuit breakers of appropriate capacity should be installed** to protect the hardware against increase in power voltage.
- Ensure the installation of **emergency power off switches** in strategic locations with adequate **labelling and shielding** to avoid accidental activation.

Equipment Maintenance

The **IT Team** shall ensure that:

- **Equipment maintenance shall only be carried out by authorized personnel.**
- **Complete and updated records of all preventive and corrective maintenance are well kept.**
- Any preventive and corrective maintenance conducted by the **supplier's personnel shall be supervised** and formal approval is obtained from the **business owner**.

NOTE: Next review cycle for this policy is **March 2027**.Management can review the 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.*