Network Security Policy
Version 8

REZOLVE.ai

Document Information

Name of the document	Network Security Policy
Release date	19-Dec-2018
Owned by	Boopathi
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	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	UpdatedDocumentInformation
6	01-Mar-2023	Reviewed and no change
7	24-Sep-2024	Updated Document Information
8	24-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022

Reviewerand Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder&CTO	Approved	24-Mar-2025

Contents

Purpose and Scope

This document defines the Network Security Policy for Rezolve.ai.
It applies to:

- All business functions and information on the network.
- The physical environment and individuals supporting the network.

This policy ensures the **confidentiality, integrity, and availability** of the network and outlines the security responsibilities across the organization.

The IT department will:

- **Ensure Availability** – Ensure the network is available for authorized users.
- **Preserve Integrity** – Prevent unauthorized or accidental modifications, ensuring accuracy and completeness.
- **Preserve Confidentiality** – Prevent unauthorized disclosure of assets.

2. Network Definition

The network includes all communication equipment such as servers, computers, printers, modems, and peripherals connected to share data, software, and resources (e.g., printers, storage devices, internet access).

3. Network Security Policy Definition

The Rezolve.ai information network will:

- Be available when needed.
- Be accessed only by legitimate users.
- Contain accurate and complete data.
- Be resilient against threats to its confidentiality, integrity, and availability.

To achieve this, Rezolve.ai will:

- Protect hardware, software, and information assets through balanced technical and non-technical measures.
- Ensure protection is effective, cost-efficient, and aligned with risk levels.
- Implement the policy consistently and in a timely manner.
- Comply with applicable laws and regulations.

Approval: This policy must be approved by the **Information Security Manager (ISM)**.

4. Security Responsibilities

- The **CEO** has delegated overall network security responsibility to the **CTO**.
- The **CISO** is responsible for implementing the policy in IT systems.

5. Risk Assessment

- Rezolve.ai will conduct regular **security risk assessments** for all business processes covered under this policy.
- These assessments will guide the appropriate security measures for protecting the network's confidentiality, integrity, and availability.

6. Physical and Environmental Security

- Network equipment must be housed in **secure, monitored environments** (temperature, humidity, power).
- Areas must have **access control**, **fire suppression systems**, and **intruder alarms**.
- **Smoking, eating, and drinking** are prohibited in sensitive areas.
- All visitors must:
  - Be authorized by the CISO.
  - Be logged (name, organization, purpose, date, time in/out).
  - Be escorted when required.
  - Be made aware of security protocols.

7. Access to Secure Network Areas

- Restricted to individuals whose roles require access.
- CISO must maintain and periodically review the access list.

8. Access Control to the Network

- Access is controlled to prevent unauthorized use.
- Access must follow a **formal registration and de-registration process**.
- Approved by department managers and the CISO.
- **Access rights and privileges** are assigned based on job roles.
- No access until CISO authorizes it.
- All users must use **individual credentials** and maintain password confidentiality.
- Access is revoked immediately when users leave or change roles.

Network Types at Rezolve.ai

1. **Office Wi-Fi** – Password-protected; access to internet and local printers.
2. **Coworking Network** – Controlled access to the internet.
3. **VPN** – Access to cloud (production/non-production) based on roles and access requirements.

9. Third-Party Access Control

- Governed by formal contracts outlining security requirements.
- All third-party network access must be logged.
- Access must be based on **role-based need** and for the required duration only.

10. External Network Connections

- All external connections require documented, approved policies.
- Must be approved by the **ISM** before activation.

11. Other Network Security Controls

- **Maintenance contracts** for network equipment must be current and reviewed.
- **Formal data/software exchange agreements** must be approved by the ISM.
- The CISO:
  - Maintains a **network fault log**.
  - Ensures **security training** for all users.
  - Supports the CTO in ensuring no security risks before operations begin.
  - Requires audits/checks of implementations against policies.
- Measures must be in place for:
  - **Virus/malware protection**
  - **Security monitoring**
  - **Configuration management**

12. Secure Disposal or Reuse of Equipment

- All data must be **securely erased** from equipment before disposal.
- Equipment may be **physically destroyed or de-gaussed** by IT staff.
- Disks sent for repair must be securely wiped in advance, where possible.

13. System Change Control

- CISO must review all security-related network changes.
- Updates to documentation, policies, and procedures must follow.
- CTO ensures selected hardware/software meets security standards.
- New network systems must:
  - Undergo acceptance testing.
  - Be evaluated for failure conditions and documented criteria.
  - Be developed and operated in separate environments.

14. Reporting Security Incidents and Weaknesses

- All security incidents must be reported and investigated according to the **organization's incident reporting procedure**.
- Reports must be directed to the **Information Security Officer (ISO)**.

The next review cycle for this policy is **March 2026**.Management reserves the right to make updates at any time depending on organizational needs.

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