ISMS Manual
Version 9

REZOLVE.ai

Document Information

Name of the document	ISMS Manual
Release date	19-Dec-2018
Owned by	Neil Dattani
Governed by	Udaya Bhaskar Reddy

Revision History

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	04-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	07-Mar-2023	Updated 5.1.1Leadership
7	24-Sep-2024	Updated Document Information
8	21-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	22-May-2026	Expanded scope to include current products; added AI/LLM-specific risk categories; added regulatory alignment to SOC 2, GDPR, HIPAA, CCPA, DPDP; reformatted stakeholder analysis; updated risk methodology with quantitative scoring; added penetration testing, and SoA review to monitoring deliverables.

Reviewer and Approver

Name	Title	Comments	Date
Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	02-June-2026

Contents

General
This ISMS manual specifies the requirements for establishing, implementing, maintaining and continually improving Information Security Management System within the context of the Rezolve.ai overall business requirements. It specifies the implementation of security controls customized to the objectives and needs of the organization.

Purpose
This information security policy is aimed to assure and communicate the management commitment and intent of supporting goals and principles for information security in line with Rezolve.ai business process. The purpose of this policy is to -

- Establish an organization wide approach towards Information Security.
- Establish controls to ensure the protection of sensitive information stored or transmitted electronically and the protection of the organization's information technology resources.
- Assign responsibility and provide guidelines to protect the organization's resources and data against misuse and/or loss.

Information security is achieved by establishing a systematic approach to manage the Information Security within Rezolve.ai and implementing a suitable set of controls that includes policies, procedures, organizational structures, and technical controls.

Regulatory and Framework Alignment

This ISMS is designed to align with and support compliance to:

- ISO/IEC 27001:2022 (primary certification standard)
- ISO/IEC 27701:2019 (Privacy Information Management, where applicable)
- SOC 2 Type II (Trust Services Criteria - Security, Availability, Confidentiality)
- GDPR (EU Regulation 2016/679)
- HIPAA (where customer data classified as ePHI is processed)
- CCPA / CPRA (where California consumer data is processed)
- DPDP Act 2023 (India)

Compatibility with other management system standards
The high-level structure and sub-clause titles of this ISMS Manual help the organization to align or integrate other related Management Systems.

Scope
The Scope of the ISMS Manual specifies the requirements for establishing, implementing, maintaining and continually improving the Information Security Management System in Rezolve.ai within the context of Rezolve.ai business operations.

This policy applies to Rezolve.ai including its affiliated entities, subsidiaries, and contracted parties. The ISMS scope explicitly covers:

- All Rezolve.ai SaaS production workloads hosted on Microsoft Azure
- All customer-facing products: Agentic Sidekick 3.0, AITSM, SearchIQ, VoiceIQ, AIOps, AI Assist for MSPs
- All integration channels: Microsoft Teams, Slack, Email, Mobile applications, web portals, and API endpoints
- All corporate IT infrastructure at Rezolve.ai offices
- All remote / work-from-home personnel accessing corporate or production environments
- All third party processors and sub-processors handling Rezolve.ai or customer data

Reference and Definitions

References and Standards	
ISO 27001:2022	Information Security Management Systems Requirements
ISO/IEC 27002:2022	Code of Practice for Information Security Controls
ISO/IEC 27017:2015	Cloud Security Controls
ISO/IEC 27018:2019	Protection of PII in public clouds
ISO/IEC 27701:2019	Privacy Information Management
NIST SP 800-53 Rev 5	Security and Privacy Controls (reference)
SOC 2 Trust Services Criteria (AICPA)	
GDPR, HIPAA, CCPA / CPRA, DPDP Act 2023	

Acronyms	Definition/Description
ISMS	Information Security Management System
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
RA	Risk Assessment
RTP	Risk Treatment Plan
SOA	Statement of Applicability
BCP	Business Continuity Plan
DR	Disaster Recovery
SLA	Service Level Agreement
ePHI	Electronic Protected Health Information
PII	Personally Identifiable Information

Context of the Organization

Understanding the Organization and Its Context
This Information Security Management System Manual reflects the Information Security Management System being practiced at all Rezolve.ai offices.

This document is for the internal users who need to practice it and for authorized external users who want to know about the Information Security Management System (ISMS) being practiced at Rezolve.ai. This Information Security Management System Manual reflects the intentions and commitment of Rezolve.ai in establishing and implementing an Information Security Management System. This manual is an auditable and demonstrable document of Rezolve.ai. It is a confidential document, only authorized persons of Rezolve.ai are allowed to access this document. Any changes to the integrity of this document have to be recorded.

Organization Setup
Top Management of the Unit consists of CEO, CTO/CISO, CRO, and Heads of Departments. The various functions are as given below:

- Product Engineering and Development
- Information Technology and Security
- Customer Success and Support
- Sales & Marketing
- Human Resources, Finance and Administration

Detailed Organization Chart of each department is maintained by central HR. IT Department of Rezolve.ai caters to IT requirements of all functions listed above and at all site locations of Rezolve.ai. IT

Department also takes the lead role in maintaining the ISMS across the organization and ensures that security requirements are addressed in all operations including internal, third party contracts and business partners and all stakeholders.

Goals and Objectives
Goals and objectives of information security policy are:

- Conformity with Rezolve.ai applicable regulations/legislation
- Enhanced information security at Rezolve.ai
- Reduced information risk to Rezolve.ai
- Avoidance of incidents detrimental to information integrity, in line with the Rezolve.ai Business objectives
- To enable the monitoring and continuous improvement of information security management
- To ensure Rezolve.ai Information security program is aligned with business needs and objectives of Rezolve.ai
- To improve the utilization of resources
- To improve risk management and resilience
- To ensure that staff are fully aware of their information security roles and responsibilities and developed to perform their roles effectively
- To develop a positive culture of information security throughout Rezolve.ai

The goals and objectives of the Information Security Policy shall be reviewed at least annually via Management Review Procedure.

External and Internal Issues:
The external and internal issues considered in the organizational context have been used to determine the scope.

External Context

Information Security is the fundamental building block for all IT services. It is also a legal and regulatory requirement that all IT Service Providers must comply with to ensure the privacy and security of customer information. Securing the integrity, availability, and confidentiality of information is a significant component of operational risk management. Therefore, computer hardware and software systems must play a major role in any IT Service Provider's operational risk profile.

Individual projects typically "own" their risks in corporate support functions such as human resources, legal, and technology. Often, they are either responsible for the offshore components of related operational risks and/or feed their associated risk information into the individual business units.

Information security leadership must be able to identify and communicate key operational risks (both threats and vulnerabilities). Measuring these risks requires estimating both the probability of an operational loss event and the potential scope of the loss.

Internal Context

Rezolve.ai is an enterprise Agentic AI SaaS company that delivers autonomous IT, HR, and shared services to global enterprises. The platform deploys specialist AI agents that automate L1 and L2 support tasks across IT, HR, and shared services domains.

Core products in scope:

- Agentic Sidekick 3.0 (autonomous AI service desk)
- AITSM (ITIL-aligned IT Service Management)
- SearchIQ (enterprise search)
- VoiceIQ (AI voice agents)
- AIOps (AI-driven IT operations)

The platform leverages multiple Large Language Models (LLMs), Retrieval-Augmented Generation (RAG), Model Context Protocol (MCP), and multi-agent orchestration. It integrates natively with Microsoft Teams, Slack, Email, and over 100+ enterprise SaaS applications.

Rezolve.ai operates on a multi-tenant SaaS model hosted on Microsoft Azure, with customer data processed under contractual Data Processing Addenda aligned with GDPR, HIPAA, SOC 2, and other applicable frameworks.

Rezolve.ai has adopted policies and procedures based on ISO/IEC 27001:2022 to manage information security. Robust risk management delivers long-term advantages, increases interested-party confidence, and protects Rezolve.ai against under-treated risks.

Understanding the Needs and Expectations of Interested Parties

Rezolve.ai shall develop, implement, maintain and continually improve a documented ISMS within the context of its overall Business activities and risks and the requirements of the interested parties.

Type	Stakeholders	Needs	Expectations	Issues
Internal	Employees	Information resources and tools to perform the work. Career growth	Learning opportunities Supportive Work environment Understanding of desired behavior Business continuity Availability of Information resources and tools	Unavailability of infrastructure Training on policies/ procedures
	Leadership(Managers, Directors)	Business continuity & growth. Framework to meet business objectives Compliance to contractual, statutory and regulatory requirements. Disaster recovery as per organizational standards and contractual requirements Brand image / corporate reputation	Risks are appropriately and continuously identified, assessed and managed. Policies, procedures, applicable laws and regulations are complied with. Objectives are achieved effectively and efficiently. The development and maintenance of effective control processes are promoted throughout.	Information Security objectives are not aligned with business objectives. Ineffective risk assessment and mitigation process. Lack of resources to implement security governance framework Lack of resources to mitigate risks. Penalties due to non-compliance to contractual, statutory and regulatory requirements Employee safety issues
	Shareholders	Business continuity & growth. Brand image / corporate reputation	Good Governance Management Accountability Regulatory Compliance Strong Corporate reputation	Brand image affected due to security risks /breaches Penalties due to non-compliance to contractual, statutory

			Transparent Reporting	and regulatory requirements Inaccurate reporting
	Internal Sales Team	Dashboards/reports to help them	24*7availability of the applications	Requirements are provided in Agile methodology. Expected turnaround time is very less.
External	Customers	Formal contract with roles and responsibilities related to security.	Information security and protection of privacy in all services Commitment to Contractual obligations and ethical principles Competitive in response to customer needs	Breach of contractual clauses related to security Penalty due to non-compliances and data breaches.
	Data Subjects (End Users of the Customers whose data is processed)	Privacy of personal data processed by AI agents; transparency over AI decisioning.	Lawful processing; right to access, rectify, and erase; protection against unauthorized AI inference; explainability.	Non-compliance with GDPR, DPDP, CCPA, HIPAA; AI bias or hallucination causing harm.
	Special Interest Groups	Information related to industry best practices/lessons learnt about information security	Sharing Information Security Best practice	Periodic updates about security best practices, new regulations not available.
	Regulatory authorities	Information about applicable regulations and appropriate time for implementing new regulations	Compliance with Laws and regulations Promoting Common interests Secured exchange of sensitive information	Non-compliance to statutory and regulatory requirements
	LLM and Cloud Sub-Processors	Compliance with their terms of service and data processing addenda.	Secure API integration; no data leakage; contractual obligations.	Sub-processor breach; model abuse; vendor lock-in.
	Investor and Board	Sustainable growth; certification readiness; risk transparency.	ISO 27001, SOC 2 Type II, and HIPAA; insurance posture.	Brand damage from a breach; valuation impact; audit findings.
	Suppliers	Fair supplier selection process and monitoring system	Fair Dealing Opportunity to grow their business Sharing Information Security best practice	Third party/Supplier risks -unauthorized disclosure, breach of trust, non- compliance to SLAs , unavailability of services
	Community/Society	Compliance to safety and environmental regulatory requirements	Safe Operations Community Support	Environmental and safety hazards caused due to Organizational

				operations

Scope of the Information Security Management System

The boundaries of ISMS in Rezolve.ai are defined in the following terms:

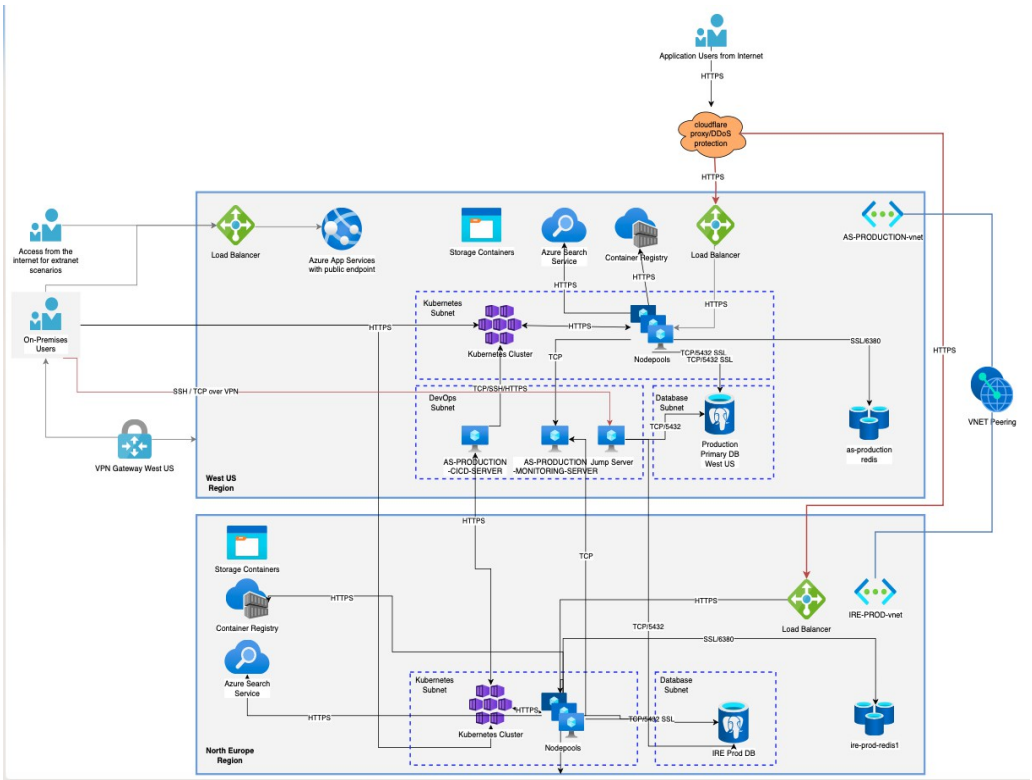
Physical Boundary:

The physical boundary is defined as Rezolve.ai office locations at: United States (Dublin and Cincinnati) and India (Dehradun, Bangalore and Chennai). All remote and work-from-home personnel accessing corporate or production environments are also within scope.

Network Boundary:

The network boundary is defined as:

- Corporate LAN at Rezolve.ai offices
- Corporate Internet gateways with secure web gateway and DNS filtering
- Site-to-site VPN and remote-access VPN endpoints
- Microsoft Azure production tenant(s) hosting Rezolve.ai SaaS workloads, including:
- Compute (Azure Kubernetes Service / Virtual Machines)
- Storage (Azure Blob, Azure SQL, Cosmos DB, and equivalent services)
- Network (Azure VNets, NSGs, Azure Firewall, Application Gateway with WAF)
- Identity (Azure AD / Entra ID for workforce and customer SSO)
- Production and Disaster Recovery Azure regions as specified in the SoA
- All API endpoints, MCP connectors, and third-party SaaS integrations within the Statement of Applicability



Scope Statement

The scope of ISMS in Rezolve.ai includes all Information and Information Processing facilities, processes, resources, and support services managed by Rezolve.ai to deliver its Agentic AI SaaS products and to ensure confidentiality, integrity, and availability of information for all interested parties.

The Information Security Management System at Rezolve.ai covers:
Core Processes: SaaS product engineering, cloud operations, customer support
Support Functions: Information Technology, Human Resources, Administration and Facilities, Legal, Finance

Scope Element	In-Scope Coverage
Location	Rezolve.ai offices at Dublin (CA,USA), Cincinnati (USA), Dehradun (Uttarakhand, India), Chennai (Tamil Nadu, India), and Bangalore (Karnataka, India). All remote and work-from-home personnel accessing corporate or production environments.
Personnel	All Rezolve.ai employees, interns, and contractors at the listed locations. Third-party personnel including physical security staff, housekeeping staff, external consultants, contract personnel, and third-party IT vendors.
Products and Services	Agentic Sidekick 3.0, AITSM, SearchIQ, VoiceIQ, AIOps, AI Assist for MSPs, and all associated APIs, MCP connectors, and integrations.
Cloud Infrastructure	Microsoft Azure production tenant(s) including compute (AKS, VMs), storage (Blob, SQL, Cosmos DB), network (VNets, NSGs, Azure Firewall, Application Gateway, WAF), and identity (Azure AD / Entra ID). Production and DR regions as specified in the SoA.
Physical Assets	Servers, workstations, laptops, mobile devices under MDM, network and security appliances (firewalls, switches, access points, VPN concentrators), encrypted backup media, printers, multi-function devices, internet links, and leased lines.
Software Assets	All software developed by Rezolve.ai (proprietary product code, internal tools, libraries). All licensed third-party software used for business operations including approved applications listed in the Approved Apps register.
Information Assets (Electronic)	Customer data, production databases, source code repositories, configuration files, system and security logs, accounting and MIS data, product artefacts, budget information, intellectual property, AI models and prompts, policies and procedures in digital form.
Information Assets (Physical)	Contractual documents, statutory records, access logs, signed agreements, and hard-copy policies or procedures.
Services	Supporting services for computing infrastructure and work environment including internet connectivity, power supplies, air conditioning, UPS, telephony, and physical access systems.
Integration Channels	Microsoft Teams, Slack, Email, Mobile apps, web portals, customer SSO (SAML / OIDC / OAuth), and all third-party SaaS integrations within the Statement of Applicability.
Scope Exclusions	Any Rezolve.ai office or group entity not explicitly listed above. Justification: these are governed by separate management systems or are not in operation; their exclusion does not affect Rezolve.ai's ability to deliver information security in conformity with ISO 27001:2022 for the certified scope.

Information Security Management System

Rezolve.ai shall develop, implement, maintain, and continually improve a documented ISMS within the context of its overall business activities and risks. The ISMS follows the Plan-Do-Check-Act (PDCA) lifecycle:

- Plan: Establish ISMS context, scope, risk assessment, and treatment
- Do: Implement and operate the ISMS controls
- Check: Monitor, measure, audit, and review effectiveness
- Act: Continually improve based on findings and changing conditions

The ISMS covers the management, operation, and maintenance of all information assets and systems supporting the design, development, delivery, and operation of Rezolve.ai's Agentic AI SaaS products and services.

Leadership & Commitment

This chapter presents the organizational initiative and commitment to effective implementation and operation of ISMS. In addition, this chapter highlights the roles and responsibilities associated with ISMS operation.

Leadership

Rezolve.ai is committed to information security and has formed an Information Security Steering Committee (ISSC) chaired by the CEO. The ISSC meets at least once every quarter
ISSC Membership:

- Chairperson: Saurabh Kumar - CEO and Chief Privacy Officer
- CISO and CTO: Udaya Bhaskar Reddy - Chief Information Security Officer and Chief Technology Officer
- Head of Engineering: Senthil Annaswamy
- Human Resources and Compliance: Aanchal Saini

Standing invitees: Internal Audit Lead, Heads of Departments and external assessors as required.

Management Commitment
Management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS as defined in ISMS documentation, by:

- Ensuring implementation of information security policy
- Ensuring that information security objectives and plans are established
- Establishing roles and responsibilities for information security and ensuring that adequate resources are available for establishing and maintaining ISMS
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law, and the need for continual improvement
- Ensuring that the desired outcomes are met after implementing ISMS
- Directing and supporting persons to contribute to the effectiveness of ISMS
- Promoting continual improvement of the ISMS
- Supporting other relevant roles as required.

ISMS Policy Statement

This policy establishes a framework of governance and accountability for information security across Rezolve.ai. It forms the foundation of the Information Security Management System (ISMS) and incorporates all supporting policies and procedures required to protect Rezolve.ai information and customer data by maintaining:

- **Confidentiality**: protecting information from unauthorized access and disclosure
- **Integrity**: safeguarding the accuracy and completeness of information and preventing its unauthorized amendment or deletion
- **Availability**: ensuring that information and associated services are available to authorized users whenever and wherever required

The policy shall be communicated to all employees, stakeholders, and third parties and will be reviewed once a year. Employees shall abide by the security policy and will, at all times, act in a responsible, professional, and secure manner.

Information Security Commitments

Rezolve.ai management commits to:

- Maintain certification to ISO/IEC 27001:2022 and SOC 2 Type II.
- Comply with applicable laws including GDPR, HIPAA, CCPA, DPDP Act, and contractual obligations.
- Maintain a Risk Acceptance threshold approved by the ISSC.
- Notify regulators and affected parties of personal data breaches within 72 hours, as required by GDPR Article 33.
- Conduct annual independent penetration testing of production SaaS workloads.
- Deliver annual information security and privacy training to 100 percent of the workforce, with role-based training for engineering and operations.
- Continually improve the ISMS based on measurable KPIs reviewed by the ISSC.

Security Governance
Information is a valuable asset that needs to be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps need to be taken to ensure that its security, integrity, confidentiality, and availability are not compromised.

The Corporate Information System Security Policy, approved by the CEO of Rezolve.ai, is the top-level Policy Document for all units/regions/divisions of Rezolve.ai. It has been published in the Corporate HRIS portal and is available at all prominent locations in Rezolve.ai offices where ISMS is implemented. It has also been published and communicated to all employees of Rezolve.ai through the Intranet, emails, posters, training, and induction programs.

Organizational Roles, Responsibilities, and Authorities

CEO - Rezolve.ai

- To approve Information Security Management System as Chairman of Rezolve.ai Information System Security Forum.
- To appoint CISO, ISSC members, and Security Organization structure.
- To review and approve objectives and targets.
- To allocate finance and resources to meet objectives and targets.
- Accept residual risks on high level on recommendations of the CISO

Chief Information Security Officer (CISO)

- Define specific roles and responsibilities of information security across Rezolve.ai.

- Coordinate with Rezolve.ai Information System Security Forum and Rezolve.ai Information System Security Coordination Team on all activities identified as part of group responsibility.
- Organize security reviews and audits, with internal and external resources.
- Ensure implementation and tracking of ISMS plan.
- Coordinate with different security coordinators within the organization.
- Organize management reviews of ISMS.
- Promote awareness amongst employees on ISMS.
- Review and prioritize significant information assets and security threats.
- Appraise incidents to the Information System Security Forum.
- Carry out RA (Risk Assessment) and prepare RTP (Risk Treatment Plan).
- Report to Head of Rezolve.ai with respect to ISMS implementation.
- Review & Approval of ISMS guidelines & procedures.
- Assessment of training requirements on information security.
- Review and approve the ISMS Manual.
- Monitor the implementation of ISMS policies and procedures.
- Review and approve the risk assessment and risk treatment plan, and accept residual risk.
- Design and deliver awareness program.
- Evaluate, implement, and ensure utilization of up-to-date security technology and techniques.
- Review and monitor information security incidents.
- Ensure ISMS is in line with new legal, administrative, and business requirements.
- Ensure that security is part of the information planning process.
- Decide specific methodologies and processes for information security (e.g., risk assessment, security classification system, etc.).
- Drive organization-wide information security initiatives.
- Assess new systems and services for security before absorbing them into the system and identify and implement appropriate security controls.
- Oversee cloud security posture management (CSPM) for the Azure production environment.
- Maintain the Statement of Applicability (SoA) aligned to ISO 27001:2022 Annex A.
- Coordinate with the CPO on privacy, breach notification, and data subject rights.
- Maintain the AI risk register and oversee responsible-AI controls including prompt-injection defence and data-leakage prevention in LLM workflows.
- Ensure customer security questionnaires and audit requests are responded to within agreed SLAs.
- Coordinate annual independent penetration testing and remediation.
- Maintain the inventory of sub-processors and review their security posture annually.

The Management Review meetings on Information Security meet at least once a year to support and supervise the activities of the CISO, taking informed decisions. Together with the CISO, it will jointly be held responsible for achieving measurable progress. The Privacy Officer is also responsible for maintaining the privacy of ePHI.

Information Security Steering Committee (ISSC)

- Conduct RA for all assets within their domains.
- Prepare and implement risk treatment plan.
- Implement ISMS policies and procedures within their domains.
- Provide necessary help in training and awareness of employees.
- Review implementation status at defined intervals.
- Ensure corrective and preventive actions for non-conformities/observations.
- Provide technical support and assistance to Information System Coordination team for implementation of ISMS policies and procedures.
- Assist CISO in preparation and review of ISMS Manual, procedures, policies, guidelines, and templates.
- Implement ISMS policies and procedures within their functional area.
- Identify and arrange for provision of training requirements to employees, suppliers, and contractors.
- Ensure corrective and preventive actions for non-conformities/observations.
- Responsible for the web content published within their functional area.

The meetings are held once every three months or on an as-needed basis.

In addition, the group helps reduce the risk of disruption of business operations by providing advice on all aspects of security, including:

- Security Awareness
- Data Confidentiality and Privacy
- **Logical Access**
- Data Communications
- Systems and Data Integrity
- Physical Security
- Contingency and Disaster Recovery Planning
- Personal and Procedural Controls

Site IT Coordinators

- Implement ISMS policies and procedures for their respective site locations.
- Identify and arrange for provision of training requirements for site employees.
- Ensure corrective and preventive actions for non-conformities/observations for their respective domain.

All Employees

- Adhere to security policies, guidelines, and procedures pertaining to the protection of sensitive data.
- Report actual or suspected breaches in the confidentiality, integrity, or availability of sensitive data to ISMS Manager.
- Use the information only for the purpose intended by Rezolve.ai.
- Maintain the confidentiality of sensitive information to which they are given access privileges.
- Take accountability for all activities performed under their user accounts and access privileges. - Complete mandatory security and privacy training as assigned.
- Never input sensitive customer or company data into unapproved AI tools or public LLM services

Other Key Personnel
The roles, responsibilities, and authorities of System Administrator, Network Administrator, Application Developers, and System Users are detailed in a 'Roles and Responsibilities' Document to be maintained. The roles and responsibilities of the BCP team are detailed in the BCP and DR (Disaster Recovery) document.

The ISMS has been designed considering the context of the organization with reference to external and internal issues and to meet the needs and expectations of interested parties. An organizational set of policies to support the top-level policy has been put in place. The organization selects and implements a set of controls to support the ISMS policies.

The selection of these is based on the following (not limited to) parameters:

- Legal and Contractual Requirements: GDPR, HIPAA, CCPA, DPDP Act, IT Act, customer DPAs, statutory record-keeping, and contractual security clauses.
- Business Requirements: Compliance with ISO 27001 and SOC 2; outsourcing and use of sub-processors; secure SDLC for SaaS product development; cloud shared-responsibility with Microsoft Azure.
- Risk Assessment Requirements: Security breaches, incidents, regulatory changes, unauthorized access, environmental threats, AI-specific risks (prompt injection, data leakage via LLM, model misuse).

Planning - Actions to Address Risks and Opportunities

When planning for the information security management system, Rezolve.ai has considered the context of the organization, determining external and internal issues relevant to the business and operations in order to:

- Ensure the information security management system can achieve its intended outcomes.
- Prevent, or reduce, undesired effects.
- Achieve continual improvement.

Information security is based on risk management. Responsible parties must manage risks to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Absolute security is unaffordable, often unachievable, and may impede business objectives and/or efficiencies.

The criteria for identification of risks are as follows:

Risk Assessment

Risk assessment is carried out with each department/function and identifies the gaps in the existing system.

- Risks that cause loss of confidentiality, integrity, and/or availability of Rezolve.ai and its customer information are identified.
- The impact of the risk and likelihood of the risks are calculated.
- **Identifying the Risk Owner**:
  Each risk owner is the person who has the most influence over its outcome. Selecting the risk owner thus usually involves considering the source of risk and identifying the person who is best placed to understand and implement what needs to be done.
- Appropriate risk management and information classification, controls, and handling procedures are defined to ensure that information security is implemented proportionately and in alignment with business requirements.

Rezolve.ai has established a risk assessment process, including risk acceptance criteria and criteria for performing information security risk assessments.
Information asset classification is as per the classification mentioned in the ISMS Induction PPT.
Please refer to the **Information Security Risk Management and Assessment Process** for further details.

Strategic Risk Management

Strategic risk management is continuously considered in business goal setting and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. The overall IT strategy includes a consistent definition of risks that the organization is willing to take.

- Realistic long-range IT plans are developed and constantly being updated to reflect changing technology and business-related developments.
- Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated as changes occur.

Risk Evaluation Criteria

Rezolve.ai uses a hybrid qualitative-quantitative risk methodology:

- Likelihood scale: 1 (Rare) to 5 (Almost Certain)
- Impact scale: 1 (Negligible) to 5 (Catastrophic), measured across confidentiality, integrity, availability, financial, regulatory, and reputational dimensions.
- Risk Score: Likelihood multiplied by Impact (range 1 to 25)
- Risk Levels: Low (1 to 6), Medium (8 to 12), High (15 to 25)

Risk Acceptance Criteria:

- Low risks: Owned and monitored; no immediate treatment required.

- Medium risks: Treatment plan within 90 days; ISSC notified.
- High risks: Treatment plan within 30 days; ISSC approval mandatory.

AI / LLM-Specific Risk Categories tracked:

- Prompt injection and jailbreak attempts against deployed AI agents
- Sensitive data leakage via LLM responses or training inference
- Hallucination leading to incorrect IT or HR actions
- Sub-processor LLM compromise
- Inappropriate use of customer data for model training
- Cross-tenant data exposure in multi-tenant inference

Information Security Objectives

Rezolve.ai has established the information security objectives at relevant functions and levels to:

- Ensure the availability of data and processing resources.
- Ensure the integrity of data processing operations and protect them from unauthorized use.
- Ensure the confidentiality of the customer's and Rezolve.ai's processed data and prevent unauthorized disclosure or use.
- Ensure the integrity of the customer's and Rezolve.ai's processed data (organization's information assets), and prevent the unauthorized and detected modification, substitution, insertion, and deletion of that data.
- Provide a comprehensive Business Continuity Plan encompassing the entire organization.
- Identify the value of information assets and understand their threats and vulnerabilities through appropriate risk assessment.
- Manage the risks to an acceptable level through the design, implementation, and maintenance of a formal Information Security Management System.
- Comply with applicable legal, regulatory, and contractual requirements.

Security Monitoring Organization Review

The company recognizes that its organization should support its commitments to customers and other stakeholders. The company has defined its organizational structures, reporting lines, authorities, and Responsibilities for the design, development, implementation, operation, monitoring, and maintenance of the system enabling it to meet its commitments and requirements as they relate to security, availability, and confidentiality. As part of the planning process Company will review its organizational structures, reporting lines, authorities, and responsibilities. Director will perform this review at least annually and whenever required.

Competency and Training Review
Company's personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining of the system affecting security, availability and confidentiality will have the qualifications and resources to fulfil their responsibilities. Company will ensure competency at the time of hiring through competency tests and interviews. New employees as well as continuing employees will be given technical and information security training. HR will perform training review quarterly and Director will monitor training status on a quarterly basis.

System Performance Monitoring
Company has put in place process and procedures to monitor its system performance and achievement of service levels. Steering committee will be provided quarterly reports of the system performance and service levels.

Resource Planning
Management will evaluate the need for additional tools and resources in order to achieve business objectives, during its ongoing and periodic business planning and budgeting process and as part of its ongoing risk assessment and management process. This will be an annual process and a part of the planning & budgeting process.

Risk Assessment
Management will review threats, vulnerabilities and risks so that controls are robust and residual risks are managed. ISC will perform the assessment and Steering Committee will review and approve it.

Access Review
Physical and logical access to all company's infrastructure and systems will be reviewed every quarterly. A report will be provided to the Steering Committee once every quarter.

Customer and Vendor Agreements
All vendor and customer contracts will contain suitable terms for protecting security, confidentiality and availability of its information. ISC will review all customer contracts for the security, confidentiality and availability terms.

Incident Tracker
All incidences will follow the formal incident response procedure. ISC will be provided reports of all open and closed incidents once every quarter. Management will ensure that corrective actions are taken as a consequence of the response.

Audits
Audits are performed by cross-functional teams. Audits will focus on information security, service level performance and process compliance. Audit reports will be submitted to Director and reviewed by the steering committee.

Third Party Service Providers
All service providers that handle Rezolve.ai or customer data, or that provide significant services, must demonstrate one or more of the following: ISO/IEC 27001 certification, or SOC 2 Type II report, or Equivalent independent attestation acceptable to the CISO.

Additional requirements: Annual security and privacy review by the CISO / CPO, evidenced in the vendor risk register. Sub-processor inventory maintained and published to customers per contractual requirements. - Right-to-audit clauses for critical sub-processors. The CISO maintains the vendor inventory and posture; the CPO reviews privacy-relevant vendors.

Security Monitoring Deliverables

Activity	Supporting Policy	Record	Frequency	Approved by	Owned by
Risk Assessment	Risk Assessment Policy	Risk Assessment report	Annual	Steering Committee	CISO
BCP plan	BCP Plan	BCP Plan document	Annual	Steering Committee	CISO
BCP Plan testing	BCP plan	BCP test Report	Annual	Steering Committee	CISO
Organization Review	Governance Document	Minutes of meeting	Annual	Director	Director
Training Review	HR Policy	Minutes of meeting	Quarterly	Director	HR
System Performance Monitoring	Customer Agreements	Performance Report	Quarterly	Steering Committee	IT
Resource Planning	Budgets& Business Plans	Resource Plan	Annually	Director	Director
Incident Tracking	Incident Response Procedure	Incident Tracker	Quarterly	Steering Committee	ISC
Access Review	Access control policy	Access Review Report	Quarterly	Steering Committee	IT
Vulnerability Management	Patch Management Policy	VA scan reports	Monthly	Steering Committee	CISO
Penetration Testing	SDLC, Network	PEN Test Report	Annual or	Steering Committee	CISO

	Security Policy		after a major release		
Vendor Risk Review	Third Party Management Policy	Vendor Risk Register	Annual	Steering Committee	CISO
Cloud Security Posture	Infrastructure Hardening Policy	CSPM Report	Quarterly	Steering Committee	CISO
SOA Review	ISMS Manual	Updated SOA	Annual	Steering Committee	CISO

Support

Personnel who have experience and expertise in the application domain and in information security concepts are assigned to manage ISMS. The competency is built through regular training courses in ISMS implementation and internal auditor certification programs.

Awareness and Training Program
Mandatory annual training for 100 percent of the workforce:

- Information security awareness
- Data privacy (GDPR, HIPAA, DPDP basics)
- Acceptable use and clean desk
- Phishing simulation participation

Role-based training:

- Engineering: Secure SDLC, OWASP Top 10, secure code review, threat modelling
- Cloud and SRE: Azure security baseline, IAM hardening, secrets management
- Customer Success and Support: Customer data handling, social engineering defence
- HR and Legal: Privacy law updates, data subject rights handling
- All staff using AI tools: Prompt injection awareness, responsible LLM use, prohibition on entering sensitive data into unapproved AI tools

Resources
The management provides resources for the implementation, maintenance, and review of the ISMS. The resources include funds, tools, human resources and any other resources that may be required for the efficient performance of the ISMS.
The CISO evaluates resource requirements for improvements in security infrastructure based on RA, review / audit records. Based on resource requirements, the Management approves/allocates the required resources.

Communication
For changes to be made in existing ISMS, the CISO consolidates the inputs and reviews the ISMS for applicable improvements and prepares an action plan and communicates the results to all interested/affected parties with a level of detail appropriate to the circumstances. All improvements should be directed towards predefined organizational Business objectives.

Rezolve.ai Management reviews the ISMS at least once in a year, or on an event-driven basis, for its effectiveness and possible improvements. This review includes assessing opportunities for improvement and the need for changes to the ISMS, including the Security Policy and Information Security objectives. Management review of ISMS is conducted in accordance with the procedure ‘Procedure for Management Review Meeting". The input to the management review of the ISMS includes but not limited to the following:

- Action items from previous ISMS reviews
- ISMS review/audit reports (Internal and External)
- Results from effectiveness measurements
- Feedback from the members of the organization. The feedback could be in the form of incidents reported or change requests. Feedback form is published in intranet for collecting feedback from the members of the organization.
- Techniques, products, or procedures, which could be used in the organization to improve the ISMS performance and effectiveness
- Vulnerabilities and threats not adequately addressed or not identified in the previous risk assessment
- Changes (e.g., environmental) that could affect the ISMS
- Recommendations for ISMS
- Organizational or business change

The output of the management review includes any decisions or actions taken in the review meeting. The decisions or actions could be in the form of:

- Improvement of effectiveness of the ISMS
- Modifications of existing procedures to respond to internal or external events that may impact the ISMS. The external or internal events may be in the form of:
    - Change of business requirements
    - Change of security requirements
    - Improvements
    - Changes in regulatory or legal requirements
    - Changes in level of acceptability of risks
    - Customer specific requirements

The results of the reviews are clearly documented. The CISO communicates output of the review and the action plan to the CEO Rezolve.ai, the CISO and the CTO through Email.

Document Information

The ISMS documentation structure:

- Level 0: ISMS Manual - describes how the ISMS meets ISO 27001:2022 requirements; details the organization's approach to management and implementation of the ISMS.
- Level 1: Policies and Procedures - the complete set of policies covering Access Control, Acceptable Use, Change Management, Incident Management, Backup, Cryptography, Data Protection, BCP / DR, Patch Management, SDLC, Third Party Management, and other domains in scope.
- Level 2: Standards, Guidelines, and Work Instructions - operational documents supporting the policies.
- Level 3: Records and Evidence - audit trails, training records, risk registers, SoA, DPIAs, RoPA, and other operational evidence.

Statement of Applicability (SoA)

The Statement of Applicability is a mandatory ISMS document under ISO 27001:2022 Clause 6.1.3 (d). It lists all 93 Annex A controls indicating applicability, inclusion or exclusion justification, current implementation status, and reference to the implementing policy or procedure. The SoA is maintained as a separate controlled document, reviewed at least annually by the CISO and approved by the ISSC.

Creating and Updating
The procedure for creation and update of documented information related to ISMS is per ‘Document Control Process’.

Control of Documented Information
All documents related to ISMS requirements are controlled as per ‘Document Control Process’. This includes:

- Review and approval of documents prior to issue or use
- Update, review and approval of necessary changes in controlled documents
- Availability of current revisions of necessary documents
- Document Name Information Security Management System Manual Document Number
- Withdrawal of obsolete documents from all points of issue or use to ensure guarding against unintended use.

- All ISMS documents are available in the central Document Management System (DMS) on a need-to-know basis with role-based access controls.
- Sensitive documents (including BCP, DR plans, incident response playbooks, encryption key management procedures, and penetration test reports) are stored in restricted-access repositories rather than published broadly. Access is granted on a need-to-know basis approved by the CISO.

Operation Planning and Control
Rezolve.ai ensures effective implementation of actions determined on the basis of Risk Analysis. Only controls applicable to achieving the security objectives of Rezolve.ai have been selected and the same have been addressed in the subsequent chapters of this manual.
Rezolve.ai has done the following activities:

- A risk assessment and treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks has been formulated. These are reviewed annually and upon material change.
- The training and awareness program has been conducted to all the employees of Rezolve.ai. Records are maintained.
- The entire operation of Rezolve.ai ISMS is managed by CISO.
- The resources required for implementing and operating the ISMS has been identified and provided by the management.
- The procedures and other controls capable of enabling prompt detection of and response to security incidents has been implemented.

Information security risk assessment
Rezolve.ai has identified the method of risk assessment which is suited to its ISMS, and the identified business information security, legal and regulatory requirements. The criteria for accepting the risk along with the acceptable levels of risk are also mentioned.
The details of the Risk Assessment (RA) process can be referred to from ‘Risk Assessment Methodology and Treatment

Risks Identification
The information assets and its owners have been identified within the scope of the ISMS. The threats to these assets have been identified and shall be regularly updated.
The vulnerabilities that might be exploited by the threats have been identified.
The impacts analysis affecting confidentiality, integrity and availability with regard to the assets have been suitably identified.

Risks Analysis and Evaluation
Loss to the business that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets have been assessed and shall be assessed regularly.
The realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls implemented shall be assessed regularly.
The levels of risks are to be analysed and categorized.
The risk acceptable or which requires treatment using the criteria established has been determined.

Information security risk treatment
Based on the Risk Assessment report, the CISO prepares the Risk Treatment Plan (RTP). The CISO obtains ISSC approval for RTP implementation and acceptance of residual risk; the CEO endorses acceptance of High-residual risks.

Identification and evaluation of the risk treatment options:

- Appropriate controls have been applied
- Risk acceptance wherever they clearly satisfy the organization's policy and the criteria for accepting the risk
- Avoiding the risks
- Transferring the associated business risks to other parties, e.g., insurers, suppliers

- Select control and controls for the treatment of risks
  Management approval has been obtained for the proposed residual risks.

Performance Evaluation
Monitoring, Measurement, Analysis and Evaluation
The monitoring and review of Rezolve.ai ISMS shall be done as follows:
Execute, monitor procedures and other controls to;

- promptly detect errors in the results of processing;
- promptly identify failed and successful security breaches and incidents;
- enable management, to determine whether the security activities delegated to people or implemented by information technology are performing as expected;
- help detect security events and thereby prevent security incidents by the use of indicators; and
- determine the actions taken to resolve a breach of security reflecting business priorities.
  Regular reviews of the effectiveness of the ISMS, which includes and not limited to meeting security policy and objectives, review of security controls, results of security audits, incidents, suggestions and feedback from all interested parties etc., shall be taken into consideration.
  Measure the effectiveness of controls to verify that security requirements have been met.
  Reference: Measurement of Effectiveness of controls sheet.
  Review the level of residual risk and acceptable risk, taking into account changes to:
- the organization
- technology
- business objectives and processes
- identified threats
- effectiveness of implemented controls; and
- external events, such as changes to the legal or regulatory environment and changes in social climate.
- Security plans to be updated to take into account the findings of monitoring and reviewing activities.
- The actions and events that could have an impact on the effectiveness or performance of the ISMS shall be recorded.
- Full ISMS internal audit covering all clauses and applicable Annex A controls is conducted at least annually.
- Risk-based spot audits (access reviews, vulnerability remediation evidence, vendor reviews, change records) are conducted semi-annually.
- Full Management Review of the ISMS is conducted at minimum annually, with quarterly tactical reviews by the ISSC.

Internal Audit

A full ISMS internal audit is conducted at least annually to verify adherence to ISO/IEC 27001:2022 and applicable Annex A controls. Risk-based targeted audits are performed semi-annually.The audits ensure that the ISMS:

- Ensures compliance with relevant legal, statutory, and contractual requirements.
- Is effectively implemented and maintained.
- Performs as expected in safeguarding the organization’s information security.

Security audits are carried out in accordance with the procedure titled **"Procedure for Internal ISMS Audits."** The audits are performed by trained personnel who do not have direct responsibility for the activity being audited.

The Chief Information Security Officer (CISO), in collaboration with the Heads of Departments (HODs), is responsible for ensuring that any identified non-conformities are addressed and closed. The CISO also oversees the planning, scheduling, organizing, and record-keeping of these audits.

Management Review

Rezolve.ai's Information System Security Forum conducts an annual review of the ISMS, or a review triggered by specific events, to assess its effectiveness and identify potential areas for improvement. This review involves:

- Evaluating opportunities for improvement.
- Assessing the need for changes to the ISMS, including the Security Policy and Information Security objectives.

Management Review of ISMS

The management review of the ISMS is conducted in accordance with the procedure **"Procedure for Management Review Meeting."** The results of these reviews are clearly documented, and records are maintained as specified. The CISO prepares an annual review plan and communicates it to the **Rezolve.ai Information Security Steering Committee**.

Overview and Purpose of Management Review Meetings

The purpose of the management review meetings is to assess the performance of the ISMS and determine whether:

- The ISMS is being used efficiently and effectively.
- Information security requirements are being met.
- Internal quality audits are effective.
- The ISMS objectives are being achieved.
- The system provides useful data for managing the business.
- The system requires any changes to align with the evolving business needs.

Responsibility

- The **CEO** and **CTO** are responsible for effectively conducting management review meetings and providing guidance for improvements.
- The **CISO** is responsible for:
    - Organizing management review meetings.
    - Reporting on the performance of the ISMS.
    - Maintaining records of management review meetings.
    - Taking follow-up actions on the meeting outcomes.

Structure & Schedule of Management Review Meetings

- The management review meetings are chaired by the **CTO** and attended by all functional/departmental heads.
- The meetings are held once every three months or on an as-needed basis.

Input for Management Review Meeting

The following inputs (agenda items) are discussed during the management review meetings:

- Review of actions taken on the last Management Review Meeting (MRM) and approval of minutes.
- Results of ISMS audits and reviews.
- Feedback from interested parties.
- Techniques, products, or procedures that could improve the ISMS.
- Performance and effectiveness of the ISMS.
- Status of preventive and corrective actions.
- Vulnerabilities or threats not adequately addressed in previous risk assessments.
- Results from effectiveness measurements.
- Follow-up actions from previous management reviews.

- Any changes that could affect the ISMS.
- Recommendations for improvement.

The **CISO** reports on the performance of the ISMS using data collected from various functions and areas. This data, along with the agenda points, is circulated to all members a reasonable time before the scheduled meeting to ensure participants are well-prepared.

On the scheduled date, the **CEO and CTO** reviews the data and analysis in the meeting and makes decisions regarding improvements (processes, products, systems, customer requirements, and necessary resources), with assigned responsibilities and target dates. A tentative schedule for the next MRM is also decided.

Output and Follow-Up

- Minutes of the meeting are prepared and circulated to all concerned.
- The ISMS team takes necessary follow-up actions and keeps the **CEO and CTO** updated on the status.

Improvement
Non-Conformity and Corrective Action

Violations of the Information Security Policy include but are not limited to:

- Non-compliance with Rezolve.ai information security policies
- Unauthorized use or disclosure of Rezolve.ai or customer information
- Loss of information or data
- Use of hardware, software, or information for unauthorized purposes including violation of laws, regulations, or contractual obligations
- Any incident that causes or may cause a breach of confidentiality, integrity, or availability
- Misuse of AI tools, including entering sensitive data into unapproved LLM services

Nonconformity and Corrective Action Process

- Step 1: Identification - via line management, security@rezolve.ai (or designated channel), or the Whistle Blowing Policy.
- Step 2: Containment - immediate measures to limit impact.
- Step 3: Root Cause Analysis - documented RCA using a recognized methodology (5 Whys, Fishbone, or equivalent).
- Step 4: Corrective Action - addresses the root cause with assigned owner and target date.
- Step 5: Verification - the CISO verifies effectiveness before closure; evidence is retained.
- Step 6: Lessons Learned - material lessons are shared organization-wide through security bulletins or training.

Disciplinary Action Violations may result in disciplinary action up to and including suspension or termination, in accordance with the Code of Conduct, Human Resource Security Policy, and applicable employment law. Civil or criminal action may be taken where warranted. The CISO consolidates improvement inputs and prepares an Improvement Plan with the ISSC. The plan is presented to management for approval and resource allocation, then implemented and tracked to closure in the CAPA register.

Continual Improvement
Management Review Meeting forum is a platform to improve the suitability, adequacy and effectiveness of the information security management system.
The CISO is responsible for continual improvement of the ISMS for suitability and effectiveness. Inputs to continual improvement can be:

- Change in security policies and objectives
- Audit/ Review Reports
- Incident Reports
- Analysis of monitored events
- Corrective and Preventive Actions
- Business Changes
- Environmental Change (New threats and vulnerabilities)
- Best practices of industry

Definitions

- **Availability** - Ensuring that authorized users have access to information and associated assets when required.
- **Business Continuity Plan (BCP)** - A plan to build in proper redundancies and avoid contingencies to ensure continuity of Business.
- **Computer Media** - Includes all devices that can electronically store information including portable hard disks, USB drives, encrypted backup media, and cloud storage volumes.
- **Confidentiality** - Ensuring that information is accessible only to those authorized to have access.
- **Continual Improvement** - Continual Improvement refers to stage improvement programs that facilitate rapid improvement phases with intermediate stabilized phases.
- **Control** - A mechanism or procedure implemented to satisfy a control objective.
- **Control Objective** - A statement of intent with respect to a domain over some aspects of an organization's resources or processes. In terms of a management system, control objectives provide a framework for developing a strategy for fulfilling a set of security requirements.
- **Disaster Recovery (DR)** - A plan for the early recovery of Business operations in the event of an incident that prevents normal operation.
- **Fall back** - Provisions to provide service in the event of failure of computing or communications facilities.
- **Information Security** - Security preservation of Confidentiality, Integrity and Availability of Information.
- **Information Security Management System (ISMS)** - The part of the overall management system based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.
- **Integrity** - Safeguarding the accuracy and completeness of information and processing methods.
- **Organization** - Refers to Rezolve.ai, unless specified otherwise.
- **Risk** - The combination of the probability of an event and its consequence.
- **Risk Acceptance** - Decision to accept risk.
- **Risk Analysis** - Systematic use of information to identify sources and estimate the risk.
- **Risk Assessment** - The overall process of risk analysis and risk evaluation.
- **Risk Evaluation** - Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
- **Risk Management** - Coordinated activities to direct and control an organization with regard to risk.
- **Risk Treatment** - Process of selection and implementation of measures to modify risk.
- **Statement of Applicability** - Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the Risk Assessment and Risk Treatment Processes. It should clearly indicate exclusions with appropriate reasons.
- **Agentic AI -** An AI system capable of autonomous reasoning, planning, and action to achieve defined goals with minimal human intervention.
- **AI Agent -** A software entity using LLMs and tools to perform tasks autonomously within defined guardrails.
- **Customer Data** - Any data, including personal data, supplied by or generated on behalf of a customer in the course of using Rezolve.ai services.
- **Data Subject -** As defined in GDPR Article 4(1).
- **DPIA -** Data Protection Impact Assessment as required by GDPR Article 35.
- **ePHI -** Electronic Protected Health Information as defined by HIPAA.
- **LLM -** Large Language Model.
- **MCP -** Model Context Protocol; a standard for connecting AI agents to external tools and data sources.

- **Multi-tenant -** SaaS architecture where multiple customers share infrastructure with strict logical separation.
- **Prompt Injection -** An attack where adversarial input causes an LLM to produce unintended or unsafe output.
- **RAG -** Retrieval-Augmented Generation.
- **RoPA** - Records of Processing Activities under GDPR Article 30.
- **SaaS -** Software as a Service.
- **Sub-Processor** - A third party engaged by Rezolve.ai to process customer personal data under contractual flow-down obligations.
- **Trust Services Criteria** - The SOC 2 framework criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Note: The next review cycle for this policy is **March 2027**. Management can review the policy anytime and make changes depending on the situation.

All documents related to policies and procedures: Any reference to Actionable Science is considered equivalent to Rezolve.ai.