ISMS Manual
Version 8

Document Information

Name of the document	ISMS Manual
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	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

Reviewer and Approver

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

Contents

Purpose
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.

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 and all parties, its affiliated partners, companies or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by Rezolve.ai. Specifically, this policy covers:

- Logical and physical boundaries of all systems
- All network, Operations area, IT systems, data and Authorized users, Public users within logical and physical boundaries.

This policy applies to all staff/ users that are directly or indirectly employed by Rezolve.ai, subsidiaries or any entity conducting work on behalf of Rezolve.ai that involves the use of information assets owned by Rezolve.ai.

Reference and Definitions

Acronyms	Definition/Description
ISO 27001:2022	Requirements of Information Security Management System

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 Rezolve.ai:

- Dehradun Office
- Chennai Office
- Bangalore Office

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, Heads of Departments, and CISO. The various functions are as given below:

- Information Technology Consulting
- Application Development
- HR and Administration
- Finance

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 a product-developing software company in the field of AITSM (AI-enabled ITSM). We have a Chat Bot (Virtual Agent) in the domain area of IT Help Desk / HR / Banking. We apply Artificial Intelligence, natural language processing, and robotics technologies at an enterprise level to automate standard repeatable tasks, enable more impactful use of data, and create tools that support employee and user productivity and decision-making—providing technical consultation and software services to our clients with utmost satisfaction.

Rezolve.ai has adopted policies and procedures based on ISO 27001:2022 as the standard to manage information security. Identification and attention to risk management would deliver tremendous long-term advantages to Rezolve.ai. Interested parties would have a higher level of confidence, and Rezolve.ai will be better protected against surprises due to inadvertently undertreated 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.

	StakeHolders	**Needs of Stakeholders**	**Expectationsfrom InformationSecurity Governance**	**Issues**
Internal	Employees	Informationresources and tools to perform the work. Careergrowth	Learningopportunities Supportive Work environment Understanding of desired behaviour Business continuity Availability of Information resources and tools	Unavailabilityof infrastructure Trainingonpolicies/ procedures

	Leadership(Managers, Directors)	Businesscontinuity& growth. Frameworktomeet businessobjectives Compliance to contractual,statutory and regulatory requirements. Disasterrecoveryas per organizational standards and contractual requirements Brand image / corporatereputation	Risks areappropriately and continuouslyidentified , assessed and managed. Policies,procedures, applicable laws and regulations are complied with. Objectives are achievedeffectively and efficiently. Thedevelopmentand maintenance of effective control processes are promoted throughout.	Information Security objectivesarenotaligned with business objectives. Ineffective risk assessment and mitigationprocess. Lack of resources to implement security governanceframework Lackofresourcesto mitigate risks. Penalties due to non-compliance to contractual,statutoryand regulatory requirements Employeesafetyissues
	Shareholders	Businesscontinuity& growth. Brand image / corporatereputation	GoodGovernanc e Management Accountability Regulatory ComplianceStron g Corporate reputation TransparentReporting	Brandimageaffecteddue to security risks /breaches Penalties due to non-compliance to contractual,statutoryand regulatory requirements Inaccuratereporting
	Internal Sales team whoareprimaryusers of the applications developedbyBusiness Process Technology team	Dashboards/reports to help them understandcurrent orders.	24*7availabilityofthe applications	Requirementsare provided in Agile methodology.Expecte d turnaround time is very less.
External	Special Interest Groups	Information related to industrybestpractices /lessonslearntabout information security	Sharing Information SecurityBestpractice	Periodicupdatesabout securitybestpractices, new regulations not available.
	Customers	Formal contract with roles and responsibilitiesrelated to security.	Information security and protection of privacyinallservices Commitment to Contractualobligation s and ethical principles Competitive in response to customer needs	Breach of contractual clausesrelatedtosecurity Penalty due to non-compliancesanddata breaches. Customerdissatisfaction.
	Regulatoryauthorities	Information about applicableregulations and appropriate time for implementing new regulations	CompliancewithLaws and regulations Promoting Common interests Securedexchangeof sensitive information	Non-compliance to statutoryandregulatory requirements

	Suppliers	Supplier selection processandmonitoring system	Fair Dealing Opportunitytogrow their business SharingInformation securitybestpractice	Thirdparty/Supplierrisks -unauthorizeddisclosure, breach of trust, non-compliance to SLAs , unavailability of services
	Community/Society	Compliancetosafety and environmental regulatory requirements	Safe Operations CommunitySupport	Environmentalandsafety hazards caused due to organizationaloperations

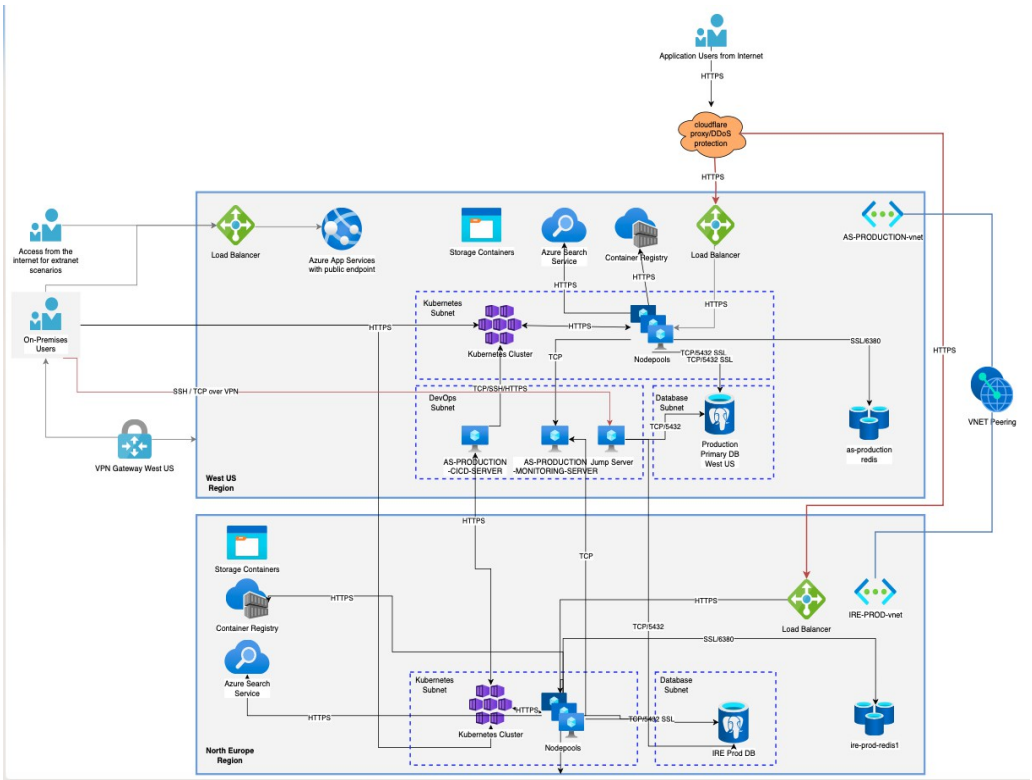
Scope of the Information Security Management System
The boundaries of ISMS in Rezolve.ai are defined in the following terms:

Physical Boundary:
The physical boundary is defined as Rezolve.ai office locations at:

- Dehradun, Uttarakhand
- Chennai, Tamil Nadu
- Bangalore, Karnataka

Network Boundary:
The network boundary is defined as:

- LAN network at Rezolve.ai offices
- Internet Gateway at the Rezolve.ai office
- All cloud operations on Azure



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 IT to provide Information & Communication services to Rezolve.ai and to ensure confidentiality, integrity, and availability in the information services extended to all interested parties.The Information Security Management System at Rezolve.ai covers:

- Core Processes
- Support Functions: Information Technology, Administration & Facility Management, Human Resources

Location	Dehradun, Chennai, Bangalore
Personnel	AllRezolve.ai.employeesattheabove-mentionedlocation.
	In addition, third party vendor are also covered under the scope of the ISMS. These users include:
	Physicalsecuritystaff
	Housekeepingstaff
	Externalconsultantsinthefacilitiesdepartment
	Contractpersonnel
	ThirdpartyITvendor
Physical assets of Rezolve.ai.areinclusivebutnotlimitedtothe following	Servers
	Workstations
	Backupdevices
	Security,Networkandcommunicationequipment
	CDs,DVDs,FloppiesandTapebackups
	Printers,scannersandFaxmachines
	Internet,Leasedlinesandcommunicationlinks
Software	AllsoftwareassetsofRezolve.ai.
The software assets of Rezolve.ai.areinclusivebutnot limited to the following:	Tools/Business applications developed by Rezolve.ai. or bought from market for internal use
Information Assets	All information assets, both in electronic media and hard copies that are in use in Rezolve.ai. are considered in the scope of the ISMS.
	The electronic information assets of Rezolve.ai. are inclusive but not limited to the following:
	Databasesanddatafilesforallbusinessactivities
	Accountinginformation
	MISreports
	Productandprocessrelatedartifacts
	BudgetInformation
	Systemsconfigurationfiles
	IntellectualpropertyofRezolve.ai.
	Operationalpoliciesandproceduresinelectronicformat
	Thepaperassets/hardcopiesofRezolve.ai.arelikethefollowing:
	Contractualdocuments
	Statutoryrecords
	Accesslogregister
	Policy/Proceduredocumentsinhardcopies
Services	Services supporting the computing infrastructure and work environment of Rezolve.ai. such as internet, power supplies, air conditioning, UPS, EPABX etc. are considered in the scope of ISMS
ScopeLimitation	The scope does not include any other offices / facilities of Rezolve.ai. and / or any other group entities of Rezolve.ai.
Furtherthescopedoesnot include:	Service delivery (core process): IFRS, Data management, Manpower outsourcing and consultancy.
	Justificationforexclusion:Theseprocessesareunderdevelopment.
	Supportprocess:Finance&BusinessDevelopment

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.

- Establish the ISMS
- Implement Corporate ISMS
- Maintain, Improve the ISMS
- Monitor and Review the ISMS

The Information Security Management System covers the management, operation, and maintenance of the information assets and information systems, as well as the associated processes that enable the development and implementation of payment and Order Management Services provided by the Business Process Technology Department in Rezolve.ai.

Leadership
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 & Commitment
Leadership
Rezolve.ai is committed to information security and has formed an Information Security Steering Committee.
The members of the Information Security Steering Committee are:

- **Saurabh Kumar**: Head of Operations, CEO & Chief Privacy Office
- **Udaya Bhaskar Reddy**: Head of Compliance, Chief Information Security Officer & Chief Technology Officer

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.

Policy

ISMS Policy Statement
This policy sets out a framework of governance and accountability for information security management across Rezolve.ai Technologies. It forms the basis of an Information Security Management System (ISMS). This shall incorporate all policies and procedures that are required to protect Rezolve.ai Technologies information 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.

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 ISSO, Information System Security Forum, and Security Organization structure.
- To review and approve objectives and targets.
- To provide finance and resources to meet objectives and targets.

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.

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 eHI.

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 Information Security Steering Committee will meet at least 4 times a year to maintain and monitor the status of implementation of ISMS in their domains.

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.
- Accept accountability for all activities associated with the use of their user accounts and related access privileges.

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 (but not limited to) parameters:

- **Legal and Contractual Requirements**: Data Protection, IT Act, Safeguarding organizational records, and Contractual Requirements.
- **Business Requirements**: Compliance with standards and security policy, Outsourcing, and use of third-party contractors.
- **Risk Assessment Requirements**: Security breaches, incidents, legislations, unauthorized access, and environmental threats.

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

These criteria are measures against which the types of impact are evaluated. The impact is rated on a scale of low, medium, and high. While calculating the risk, the probability of exploitation of a particular vulnerability along with the impact is also considered.
Risk is further categorized into three levels: Low, Medium, and High. A risk level matrix is used to determine the risk level.

Information Security Objectives and Planning to Achieve Them

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
Company will ensure that all service providers who provide significant services will be SOC2 compliant, ISO 27001 certified or any other certification. Information Security Champion (ISC) will monitor such certifications.

Security Monitoring Deliverables

Activity	**Supporting Policy**	**Record**	**Frequency**	**Approved by**	**Owned by**
Risk Assessment	Risk Assessment Policy	Risk Assessment report	Annual	Steering Committee	ISC
BCP plan	BCP Plan	BCP Plan document	Annual	Steering Committee	ISC
BCP Plan testing	BCP plan	BCP test Report	Annual	Steering Committee	ISC
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

Support

Competence

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

When the required levels of skill and expertise are not available, trainings are provided to ensure skill / knowledge enhancement as per the organization training process. The ISMS training is an integral part of training curriculum of HRD.

Identifying what training is needed, and how frequently, for specific positions.
Identifying qualified individuals/agency to conduct the training program.
Organizing the training program.
Maintaining attendance records, course outlines and course feedback of all trainings conducted.
Rezolve.ai. maintains records of all training programs organized by it.

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 ISSO communicates output of the review and the action plan to the CEO Rezolve.ai., the CISO and the CTO through Email.

Documented Information
General
The documentation structure and components of ISMS documentation is as detailed below:

- Level - 0 ISMS Manual (ISMS) - This document describes how the defined ISMS meets the requirements of information security. The document details the organization's approach towards management and implementation of ISMS.
- Level - 1 Policies and Procedures - A complete set of supporting technical policies identified and defined by the organization, and within the scope of ISMS.

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 security documents are available on the Intranet for reference and use based on need-to-know requirements. This excludes all the documents related to Business Continuity Management Process.

Operation
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.
- The training and awareness program has been conducted to all the employees of Rezolve.ai. Private Limited.
- 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 Recovery Time Point. The CISO then obtains approval of the CEO for Recovery Time Point implementation and acceptance of residual risk.

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.
- Internal ISMS audit every 6 months or annually.
- Management review of the ISMS is done annually, to ensure that the scope remains adequate and improvements in the ISMS process are identified.
- 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.

Internal Audit

Internal ISMS audits are conducted at least once every six months to verify adherence to the Information Security Management System (ISMS). 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 **COO** 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 **COO** updated on the status.

Improvement
Non-Conformity and Corrective Action
Violations of Information Security Policy may include, but are not limited to:

- Non-compliance with the requirements of Rezolve.ai. information security policies.
- Unauthorized use of Rezolve.ai. information or any customer information held by Rezolve.ai. including unauthorized disclosure of data.
- Loss of information and data pertaining to Rezolve.ai. or its customers.
- Use of hardware, software or information for unauthorized or illicit purposes, which may include violation of any law, regulation or reporting requirements of any law enforcement agency or government body.
- Any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or technical information assets of Rezolve.ai.

Non-compliance with the Information Security Policy would result in disciplinary action that may include, but is not limited to, the following:

- Suspension and / or termination.
- Civil and / or criminal prosecution.

The CISO compiles all inputs identified for improvements and prepares an Improvement Plan with the help of the Rezolve.ai. Information System Security Steering Committee. This plan is presented to the management for approval and resource allocation. The plan is created, implemented, and tracked.

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. This includes but not limited to diskettes, CD's, tapes, cartridges, and portable hard disks.
- **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.

Note: The next review cycle for this policy is March 2026. 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.