Change Management Policy

Version 9

REZOLVE.ai

Document Information

Name of the document	Change Management Policy
Release date	19-Dec-18
Owned by	Mayank Baghel
Governed by	Mr. 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	03-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	01-Mar-2023	Reviewed and no change
7	13-Sep-2024	Reviewed and no change
8	21-Mar-2025	Changes update related to requirement clause 6.3 and as per migration from ISO27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and no change

Reviewer and Approver

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

Table of Content

Purpose and Scope

Purpose

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Therefore, changes/addition/removal of information processing facilities and systems shall be controlled. Formal management policy will ensure satisfactory control of all changes to equipment, software or procedures.

Scope

Change management process is designed to control the implementation of all changes made to Software any device, application, production environment and infrastructure.

All changes to ISMS will be carried as per this document.

This procedure is applicable whenever a change is affected in any information processing facilities of Rezolve.ai or changes to process/procedure documentation.

Objectives

- All changes are properly recorded, documented, analyzed and communicated to concern teams internal and external.
- Details of all Changes are tracked and stored for the purpose of historical trending and reporting. T
- The proper analysis and testing is performed to assess the need for a change versus the potential impact of the change.
- No change is executed without first being properly planned, documented, peer reviewed, tested and approved.
- Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.

Roles and Responsibilities

Change Advisory Board (CAB)

The Leadership Team will act as a Change Advisory Board. This group is responsible for final review and approval or rejection of all RFC's. All approvals are obtained and tracked on the Jira ITTracker project for changes that need approvals.

The CAB has the authority to do any of the following -

- Cancel or rejects changes
- Approve RFC's as presented
- Re-assess the risk level of a change
- Re-assess the impact of a change
- Request additional information prior to approval

Note - Emergency RFC's due to their urgent nature, may be performed without prior review by the CAB only if written approval from CTO.

Change Manager

Respective functional Team Leads are Change Managers.

- Responsible for the overall facilitation of the Change Management process.
- Facilitate the resolution of any schedule conflicts that may arise.
- Maintain the run book for executing the change.
- Grant access to required change infrastructure.
- Ensure any non-standard notification of user communities or POC is performed.

Change Approver

Functional Head is the Change approver who provides the first level approval to a RFC, allowing it to go before the CAB for review. CTO is the final approver for all major changes to product and services and system infrastructure.

- Review or draft all RFC's.
- Ensure all necessary communication, coordination, documentation and testing has been completed properly on all RFC's prior to approval.
- Approve all RFC's prior to them being submitted for review to the CAB.

Change Assignee

The Change Assignee is the person who is the owner of the Change. This person will work with the Change Requestor to gather the appropriate information required to create and request the RFC.

- Creation of the RFC including Peer Review of the Change.
- Communication and co-ordination of change testing and implementation.
- Communicate with Change Requester to resolve any questions or problems with a proposed change.
- Update Change requester to provide status on the implementation.
- Update closure status in CMS.

Change Requester

The change requester is the person who initially request that a change take place.

- Responsible for initial escalation / request for change
- Provision of business and technical requirements to the Change Assignee.
- Resolution or escalation of Change issues.
- Provide input in the assessment of the change's level of risk.
- Provide input in the assessment of change's level of impact.
- Facilitate any required client testing before, during or after change execution.

Policy Standards

Types of Change Requests

The following table lists different types of change requests

Cluster	Type of Change Request
Hardware	New systems and improvements to existing systems and infrastructure.
Software	Changes to the existing software / application, patch updating, release of new version, installation.
Operations	Changes that affect or improve day-to-day operations of the technology.
Process	Changes to process or updating of documents

Change Classification

The following table lists the various PRIORITY of a change request

Priority	Priority Definition
Highest	Causing loss of service or severe usability problems to a large number of users, a mission-critical system, or some equally serious problem. Immediate action required. Emergency meetings of the ISF may need to be convened. Resources may need to be immediately allocated to deploy such authorized changes.
High	Severely affecting some users or having an impact upon a large number of users. To be given highest priority for change building, testing, and implementation resources.
Medium	No severe impact but rectification of an incident cannot be deferred until the next scheduled upgrade
Low	A change is justified and necessary, but can wait until the next scheduled release or upgrade. To be allocated resources accordingly.

Category of Change

Change category needs to be set based on the following definitions:

Category	Category Definition
Major	Involves potential impact on the highest percentage of users or a business-critical system. The change may be new technology or a configuration change. It may involve downtime of the network or a service.
Significant	Affects a high percentage of users. The change is a nonstandard change, such as a new product, new users, or network changes, and may involve downtime of the network or a service.
Minor	Affects a smaller percentage of users and risk is less because of the organization's experience level with the proposed change.
Standard	Affects the smallest percentage of users and has a set release process.

Change management procedure details how a change is carried out. It includes how a change is raised, classified, authorized, how the change implementation is planned & deployed and the backup plan if the change does not serve the intended purpose.

Roles & Responsibilities

Role	Responsibility
Employees / Users	Request for change
Respective Department Head / Project Manager	Classify and approve the change request, Define Roll back plan
Infrastructure Head	Approve the change request, Impact Assessment, Development, Change Review
IT team	Change Deployment, Change Communication Routine Change Management, Change Review

Change Management Process

Change Request

Initiation

- A request is initiated when a new feature or modification or a deletion in existing feature is requested or suggested by the users, or any team members from the development team or management, or by any source.
- A request may also be initiated as a part of corrective or preventive action plan prepared based on analysis of high severity incidents.

Request Form

- All changes will be tracked via a Request for Change (RFC). RFC's will be entered into and managed through a Change Management System, which will be created to ensure Changes are centrally tracked. These are tracked in ITTrackers in Jira.
- Employees make also make a request for any change through email to IT team keeping respective managers/Department head in loop.
- The change request must be authorized by the respective department head / project manager.

Change Classification

- The Department Head / Project Manager must understand the change requested and classify the change based on its priority and category.

Change Review and Authorization

- While approving the change request, the approving authority should consider the following:
- Impact of the change. For change categorized as significant or major, the ISF head / Department Head / Project Manager (as appropriate) should carry out an impact assessment to understand the overall impact if the change is implemented.
- Determine potential impact on Service level
- Effort and resources required to implement the change.
- Implementation steps, target completion date.
- Roll back plan and time required to implement it.
- If the change would have group / organization wide impact the request should be forwarded to ISF head.
- The ISF head should assess the request for its priority. This should include the C-I-A attributes.
- Wherever required, tests should be carried to assess the impact of changes before authorization.
- Once it is decided that change is required, the change request should be authorized by ISF head and in case of major changes the decision will be taken by the ISF.
- Once it is decided that change is required, the change should be authorized, else the change should be rejected and reason should be given to the requestor.

Change Development

After a request for change has been approved, it moves into the change development phase. This phase is concerned with the steps necessary to

- Plan the change
- Develop technical configurations
- Develop the functional deployment criteria
- Draft the roll back plan
- Decide on the timelines for implementation, roll back, lead time before rolling back etc
- Criteria for deploying into operations

Testing for Software Code Only

- Prior to deployment, a planned change should be scheduled for test environment, Conduct User Acceptance Tests.

- Test plans and test data are created and used in required system and regression testing. Test plans and test data are reviewed and approved by the tester prior to and at the completion of testing and reviewed by the concerned HOD prior to newly developed or changed software being authorized for migration to production. Security vulnerability testing is included in the types of tests performed on relevant application, database, network, and operating system changes.
- System and regression testing is prepared by the testing department using approved test plans and test data. Deviations from planned results are analyzed and submitted to the developer.
- Code review or walkthrough is to done for high impact changes that meet established criteria (that mandate code reviews and walkthroughs) and these are performed by a peer programmer that does not have responsibility for the change.
- Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.
- Logical access controls restrict the ability to migrate between development, test, and production to change deployment personnel.

Change Deployment

- Changes are deployed into operation only after the Change Owner / Project Manager / Department Head ensures that the criteria for functional deployment (as identified during the change development phase) are met.
- The change is released to the production environment
- In order to determine whether the deployed change has been effective and has achieved the desired results, it is necessary to monitor the change in the operational environment. For a small change, this may consist of checking on the desired functionality. For a larger change, it might require the monitoring of network and server information, performance data, event logs, or response times etc.
- A successful validation should result in completion of the change. If the change cannot be validated the environment should be reverted to its prior stable state.

Roll Back

- If the change has not met the objectives and is affecting users or parts of the infrastructure adversely, then a decision needs to be made about rolling back and removing the change from the operational environment.
- In such cases, based on the timelines identified during the Change Development Phase, the roll back plan should be implemented.

Change Review

- Following a successful release and deployment into the operation or as in the case of a standard change, just a deployment into operation, review must be conducted to establish whether the change has had the desired effect and has met the requirements from the original request for change.

Emergency Change

- Change requests prioritized as "EMERGENCY" may be scrutinized by ISF head and should be approved, if found suitable.
- In cases where the situation cannot wait for approval even from ISF head, the change requestor / change implementer may proceed with deploying the change and he / she would be responsible for effecting the change.
- Situations which would qualify for effecting Emergency changes without proper approval could be - major virus attack, hacking attempt, simultaneous failure of redundant systems etc
- These should subsequently be discussed in the ISF and with assessment of security aspects and any additional actions taken up as required and approved by ISF.

Routine Change Management

These are changes (standard category) which are of routine in nature and which need not be brought under the detailed change control procedure. A list of such changes made should be maintained and ISF head should scrutinize this as and when needed.

Change Communication

- Once the change development is completed and deployed, change owner should intimate all the relevant stakeholders about the change deployment.
- All planned changes that will impact, or have the potential to impact a production service must be communicated to the Customers or users prior to execution.

NOTE - Next review cycle for this policy is March 2027. Management can review policy any time and can make changes depending on the situation.

***** All documents related to policies and procedures any reference to Actionable Science labs Private Limited is as good as Rezolve.ai