Incident Management Policy
**Version 9**

REZOLVE.ai

**Document Information**

| | |
|---|---|
| **Name of the document** | Incident Management Policy |
| **Release date** | 19-Dec-2018 |
| **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 | 02-Mar-2023 | Reviewed and no change |
| 7 | 24-Sep-2024 | Updated Document Information |
| 8 | 24-Mar-2025 | Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022 |
| 9 | 29-May-2026 | Reviewed and updated |

**Reviewer and Approver**

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

**Table of Contents**


1. Incident Management Overview 2
2. Incident Definition 2
3. Classifying the Incident 2
4. Escalation and Support 2
5. Incident Management Process 2
6. Incident Logging 2
7. Incident Classification 3
8. Incident Analysis, Resolution, and Closure 3
9. Incident Process Control 3
10. Knowledge Base 3

**Incident Management Overview**

**Incident Definition**
An incident is an unplanned interruption to or quality reduction of a service. The service level agreements (SLA) define the agreed-upon service level between the provider and the customer. An incident interrupts normal service; incident management restores IT services to normal working levels.
Incidents cover the following:

- Administrative Incidents
- HR Incidents
- Security Incidents
- IT Incidents
- Operational Incidents
- Customer service related Incidents
- Cloud Security Incidents
  Product incidents are tackled as part of the product support process and are not in scope of this document.

**Classifying the Incident**
It is common for multiple incidents to exist in parallel, making it necessary to define levels of priority when resolving them. The level of priority is essentially based on two parameters:

- **Impact**: This determines the importance of the incident depending on how it affects business processes and/or the number of users affected.
- **Urgency**: Depends on the maximum delay the customer will accept for the resolution of the incident and/or the level of service agreed in the Service Level Agreement.
  Secondary factors, such as the expected resolution time and the resources necessary, also need to be taken into account: "simple" incidents will be dealt with as soon as possible.
  Depending on the priority, the necessary resources will be assigned to resolve the incident. The incident's priority may change during its life cycle. For example, a temporary solution may be found that restores acceptable levels of service and allows the closure of the incident to be delayed without serious repercussions.

**Escalation and Support**

- **Functional escalation**: The support of a higher-level specialist is needed to resolve the problem.
- **Hierarchical escalation**: A manager with more authority needs to be consulted to take decisions that are beyond the competencies assigned to this level, for example, to assign more resources to resolve a specific incident.

**Incident Management Process**

- **Tools/Applications used for Incident Management**: An Application for Incident Management has made available a Jira project that can be tracked and logged from incident raising to resolution.

**Incident Logging**
The essential first step in managing incidents correctly is to receive and log them. Incidents may be reported from various sources, such as users, application managers, or technical support, among others.
Incidents should be logged immediately as it is much more difficult to log them later and there is a risk of new incidents emerging, causing the process to be postponed indefinitely.

**Incident Logging Details**

- **Commencing handling of the incident**: The Service Desk must be able to evaluate whether the service required is included in the customer's Service Level Agreement in the first instance and if not, forward it to a competent authority.
- **Checking that the incident has not already been logged**: It is common for more than one user to report an incident, so it is necessary to check to avoid unnecessary duplication.
- **Assigning a reference**: The incident will be assigned a reference number to uniquely identify it in both internal processes and when communicating with the customer.
- **Initial logging**: The basic information needed to process the incident (time, description of the incident, systems affected, etc.) has to be entered on the associated database.
- **Supporting information**: Any relevant information for the resolution of the incident that may be asked for from the customer using a specific form.

- **Incident notification**: In those cases where the incident may affect other users, these should be notified so that they are aware of how the incident may impact their usual workflow.

**Incident Classification**
The main aim of incident classification is to collect all the information that may be used to resolve it. The classification process should implement at least the following steps:

- **Categorization**: A category is assigned (this may in turn be subdivided into several levels) depending on the type of incident and the work group responsible for resolving it. The services affected by the incident are identified.
- **Establishing the level of priority**: The incident is assigned a level of priority, based on predefined criteria, depending on its impact and urgency.
- **Monitoring the status and the expected response time**: An incident is associated with the incident (for example, logged, active, suspended, resolved, closed) and the resolution time for the incident is estimated based on the relevant Service Level Agreement and the priority.

**Incident Analysis, Resolution, and Closure**
In the first instance, the incident is examined with the aid of the Knowledge Base to determine if it can be matched with any incident that has already been resolved and the assigned procedure applied.
Track the issues on a periodic basis so all incidents are taken care of within defined times.
Throughout the life cycle of the incident, the various agents involved must update the information stored in the databases so that all the levels involved have complete information on the incident's status.
If necessary, a Request for Change (RFC) may be raised. If the incident is recurrent and no definitive solution is found.
Once the incident is solved, the following steps should be taken:

- Confirm with users that the solution is satisfactory.
- The resolution process should be added to the Knowledge Base.
- The incident should be reclassified if necessary.
- The incident should be closed.
- Communicate system change-related incidents to internal & external users via email.
- Dev-ops Engineering reviews the incidents and tries to resolve the same. If not resolved, escalate the same to a senior engineer.
- If there is an outage, communicate the same to the concerned team or management by email. After closure, an update is sent to the concerned team or management by email.

**Incident Process Control**
Preparing reports correctly is an essential part of the Incident Management process. These reports must provide essential information, for example, for:

- **Service Level Management**: It is essential that customers have timely information about the level of compliance with Service Level Agreements and that corrective measures are taken in the event of non-compliance.
- **Monitoring the performance**: Determining the degree of satisfaction of the customer from the service delivered and supervising proper functioning of the first line of support and customer care.
- **Optimizing the allocation of resources**: Managers need to know if the escalation process has followed the established protocols faithfully and if duplication has been avoided in the management process.
- **Identifying mistakes**: It may happen that the specified protocols are not right for the organization's structure or the customer's needs, meaning that corrective measures need to be taken.
- **Availability of Statistical Information**: Which may be used to make future projections about the assignment of resources, additional costs associated with the service, etc.

**Knowledgebase**
Also, proper Incident Management requires infrastructure enabling it to be implemented correctly. This includes:

- RCA is captured on the incidents. If the runbook needs correction or updates, these are added as tasks for the incident and tracked.
- A knowledge base (Knowledge Base) allowing new incidents to be compared with logged and resolved incidents. An up-to-date (Knowledge Base) allows:
    - Unnecessary escalation to be avoided.
    - Engineers' know-how to be turned into a lasting asset for the company.
    - Some or all of this data to be made directly available to customers (in the form of an FAQ) on the Extranet. This can mean that sometimes the user does not even need to report the incident.
      To monitor the process correctly, it is indispensable to use metrics allowing the functioning of the service to be evaluated as objectively as possible. Some of the key aspects to consider are:
- Number of provisionally classified incidents and their priorities.
- Resolution times classified according to the incidents' impact and urgency.
- Level of compliance with the Service Level Agreement.
- Associated costs.
- Use of available resources in the Service Desk.
- Percentage of incidents, classified by priorities, resolved in the first instance.
- The customer's level of satisfaction.

**NOTE**: Next review cycle for this policy is March-2027. Management can review policy at any time and make changes depending on the situation.
All documents related to policies and procedures: Any reference to Actionable Science is as good as Rezolve.ai.