Patch Management

Version 9

Document Information

Name of the document	Patch Management
Release date	19-Dec-2018
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

RevisionHistory

Version No	VersionDate	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	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	04-June-2026

Table of Contents

Rezolve.ai is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. Rezolve.ai has an obligation to provide appropriate protection against malware threats, such as hacking, viruses, Trojans, and worms, which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

1. Purpose

This document describes the Information Security requirements for maintaining up-to-date operating system security patches on all Rezolve.ai-owned and managed workstations, firewalls, and servers.

Scope

This policy applies to workstations, firewalls, or servers owned or managed by/for Rezolve.ai. This includes systems that contain company or customer data owned or managed by/for Rezolve.ai, regardless of location.

The following systems have been categorized according to management:

- Cisco firewalls managed by Rackspace
- Microsoft Windows servers managed by Rackspace
- Workstations managed by IT Infrastructure Team

2. Policy

Workstations, firewalls, and servers must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all firewalls, laptops, desktops, and servers owned and managed by Rezolve.ai Systems and Rackspace.

The production servers are all hosted on Azure and are managed by Azure Managed Services.

Workstations

Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations owned by Rezolve.ai.

Servers must comply with the minimum baseline requirements that have been approved by IT Infrastructure. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Rezolve.ai's asset and the data that resides on the system.

Monitoring and Reporting

Active patching teams noted in the **Roles and Responsibility** section (5.0) are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit upon request.

Vulnerability scans must be conducted on a weekly basis to check that the patches are current.

Exceptions

Exceptions to the patch management policy require formal documented approval from the EVP, Rezolve.ai Systems. Any firewalls, servers, or workstations that do not comply with policy must have an approved exception on file with the EVP, Rezolve.ai Systems.

3. Definitions

Term	Definition
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth

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