Infrastructure Hardening Policy

Version 9

REZOLVE.ai

Document Information

Name of the document	Infrastructure Hardening Policy
Release date	19-Dec-2018
Owned by	Mayank Baghel
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	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 Content

Purpose and Scope

Overview

Hardening is the process of securing a system by reducing its surface of vulnerability. The more functions a system performs, the larger its vulnerability surface. By removing any software, user accounts, or services that are not required for the system's intended function, the number of possible attack vectors is minimized.

System hardening is often vendor-specific, as different vendors install different components by default. Additionally, obfuscation—making it difficult for an attacker to identify the system—reduces the likelihood of a successful attack by preventing exploitation of known weaknesses.

Purpose

This policy defines the procedures to be followed for infrastructure hardening at Rezolve.ai. The goal is to restrict computing environments to the minimum required services and software necessary for operation.

This policy applies to the configuration of all desktops and laptops used within Rezolve.ai, ensuring systems are set up with only essential software and services.

Scope

This policy applies to all components of the information technology infrastructure, including:

- Computers
- Servers
- Application Software
- Peripherals
- Routers and Switches
- Databases
- Telephone Systems

Policy Standards

General Standards

- All desktops and laptops shall be hardened using predefined security configurations before deployment.
- These configurations must be documented, and the checklist must be signed off by the responsible administrator.
- The IT staff is responsible for maintaining system hardening and ensuring changes do not compromise the secure configuration.
- Vanta software is subscribed and configured to detect and report deviations on laptops and systems.

Risks Addressed

- Unpatched and poorly configured systems increase the risk of system unavailability due to attacks or malware.
- Advertising software versions (e.g., via web or email servers) helps attackers identify potential weaknesses.
- Unnecessary services or open ports offer additional avenues for attack.

Hardening Practices

Production Systems

- **Remove Unused Software**: Eliminate software packages not required for system functionality.

- **Disable or Remove Unnecessary User Accounts**: Remove unused default accounts, change default passwords, and consider renaming built-in accounts.
- **Disable or Remove Unused Services**: Shut down or uninstall unnecessary background services.
- **Apply Patches**: Systems must be fully patched with current service packs and security updates.
- **Perform Vulnerability Scans**: Use an approved scanner to identify vulnerabilities. Remediate all critical issues before moving the system to production.

Hardening Requirements

- Only software approved by the Architecture team is permitted for installation.
- Unauthorized or non-essential software/services will be removed or disabled.
- Vulnerability scanning tools will be configured to automatically remove unauthorized software.
- **SYSKey [DEPRECATED — removed from Windows by Microsoft in version 1709, October 2017]** passwords will be implemented on all laptops.
- The boot sequence will be locked to prevent unauthorized boot from external media.
- Devices will be built from a standard image. Any changes require a documented business justification.
- Anti-virus and anti-spyware software must be installed and configured for automatic updates.
- A local firewall will be enabled and configured to only allow approved inbound traffic.
- Devices will be scanned every 3 months for vulnerabilities. Findings will be documented and resolved.
- Systems must be patched per the Technical Vulnerability and Patch Management Policy.

System Security Patches and Standard Build

- All security patches must be applied to all laptops and desktops.
- Only the standard Rezolve.ai build (per the “Rezolve.ai Software Standard List”) may be used unless an exception is granted.

Anti-Virus Application

- An anti-virus application with updated virus signatures must be installed on all systems.
- Updates must be synchronized regularly from the anti-virus server.

Group Policies for Production Desktops

- **Configuration Restrictions**: End users cannot change system configurations.
- **Software Installation Restrictions**: Users must obtain IT approval before installing any software.
- **Removable Media Controls**: USB ports, CD-ROMs, and floppy drives will be disabled.
- **Policy Violations**: Disciplinary action per the HR Security Policy will apply to users who breach these security measures.

Storage of Files

- Users must not store files locally on production systems.
- Personal files such as music, movies, or unofficial content must not be stored on Rezolve.ai systems or network shares.

Failure to Comply

Violations of this policy will be handled in accordance with Rezolve.ai disciplinary procedures. Sanctions may include:

- Disciplinary action under company policy
- Termination of employment

- Legal action as per applicable laws and contractual obligations

Appendix: Approved Software List

1. Open-source software not used for commercial purposes (e.g., under Apache 2.0 or MIT licenses). For other licenses or commercial use, seek IT approval.
2. Software subscribed by Rezolve.ai (e.g., Figma, Office 365), whether user-based or seat-based.

Note: The next review cycle for this policy is scheduled for **March 2027**. Rezolve.ai management reserves the right to review and revise this policy at any time, depending on the circumstances.

All documents related to policies and procedures—any reference to Actionable Science is as good as Rezolve.ai