Vulnerability Disclosure Policy

Rezolve.ai and Rapport

Actionable Science, Inc. ("Rezolve.ai") is committed to the security of its products and its customers' systems. This policy sets out how to report a security vulnerability, the testing we authorise, and how we handle and disclose reports.

1. Scope

In scope	Examples of issues we want to hear about
rezolve.ai, rapport.rezolve.ai and subdomains operated by Rezolve.ai	Authentication and session flaws; injection; cross-site scripting; access-control and tenant-isolation failures
Rezolve.ai platform web, mobile and chat applications	Exposure of another tenant's data; privilege escalation between roles
Rapport Console, gateway and APIs	Bypass of multi-factor authentication, Approval Controls or audit logging; abuse of Enrollment Tokens or API keys
Rapport Agent for Windows, macOS and Linux (preview)	Local privilege escalation; bypass of signature, certificate or policy verification; tampering with updates; command execution outside command classification
Rapport AI Features	Content on a device or in the Console that causes the AI Assistant to run a command without the required approval, or to disclose data outside the tenant

Out of scope

- Denial-of-service, load or volumetric testing.
- Social engineering, phishing, or physical attacks on our offices or staff.
- Infrastructure operated by third parties, including Supabase, Vercel, Microsoft and Anthropic; report those to the provider.
- Devices, tenants or data belonging to our customers.
- Findings from automated scanners without a demonstrated, exploitable impact.
- Missing security headers, cookie flags or TLS settings without a demonstrated impact; clickjacking on pages without sensitive actions; self-XSS.
- Model outputs that are inaccurate or objectionable but have no security impact.

2. How to report

Email **security@rezolve.ai**. If you need an encrypted channel, say so in your first message and we will provide one. Please include:

- the affected product, component, URL or Agent version;
- a description of the vulnerability and its potential impact;
- step-by-step reproduction instructions and any proof-of-concept;
- your assessment of severity (CVSS, if available);
- whether you wish to be credited, and the name to use.
- Do not include passwords, access tokens, unrelated Personal Data or complete customer datasets in your report.

3. Testing rules

- Test only against tenants, accounts and devices that you own or are explicitly authorised to test. You may use a Rapport free trial and enrol your own devices for testing. If you need more time or devices, contact security@rezolve.ai. Testing involving another customer’s environment or data, or any testing outside this policy’s scope, requires our prior written authorisation and any necessary authorisation from the affected owner.

- Access only the minimum data needed to demonstrate the vulnerability. If you encounter data belonging to others, stop, do not retain it, and report it immediately.
- Do not use a vulnerability to execute commands on, access or alter any device you do not own.
- Do not degrade the availability of our services or disrupt other users.
- Do not exfiltrate data, install persistent access, or pivot to other systems.
- Keep vulnerability details confidential until 30 days after we release a fix, or 90 days after your report, whichever is later, unless we agree otherwise.

4. Our commitments

Stage	Target
Acknowledge receipt	Within 3 business days
Triage, validate and assign severity (CVSS v3.1 or v4.0)	Within 10 business days
Status updates	At least every 30 days until resolution
Remediation – Critical	Within 30 days of validation
Remediation – High	Within 60 days of validation
Remediation – Medium and Low	In a scheduled release

For vulnerabilities in the Rapport Agent, we may release a fixed Agent version and notify customers to adopt it through their release settings. We report actively exploited vulnerabilities to authorities where required by law. Please note that the above table includes targets which are not inherently contractual commitments.

5. Disclosure

- We coordinate public disclosure with the reporter.
- We publish security advisories for vulnerabilities that affect customers, including affected and fixed versions, and request CVE identifiers where appropriate.
- With the reporter's consent, we credit the reporter in the advisory.

6. Safe harbour

If you make a good-faith effort to comply with this policy, we will consider your research authorised. We will not initiate or support legal action against you, including under the US Computer Fraud and Abuse Act, the anti-circumvention provisions of the US Digital Millennium Copyright Act or equivalent laws, for research conducted in accordance with this policy. If a third party brings legal action against you for such research, we will make it known that your activities were authorised by us. This safe harbour does not authorise unlawful access, access to another customer's data or testing of third-party infrastructure, and does not extend to activity that breaches this policy or applicable law.

7. Rewards

We do not currently operate a paid bug bounty programme.

8. security.txt

Our security.txt files, which point to this policy and to security@rezolve.ai, are published at https://www.rezolve.ai/.well-known/security.txt and https://rapport.rezolve.ai/.well-known/security.txt.