Araxxe Information Security Management System

Responsible Vulnerability Disclosure Policy

Version: 1.1

araxxe

www.araxxe.com

Table of Contents

1. Executive summary

This document is a Responsible Vulnerability Disclosure Policy for the Araxxe service platform.

It aligns with the ISO 27001 Annex A Control 8.8 (management of technical vulnerabilities). Its objective is to setup a proactive process for handling security flaws of the Araxxe platform discovered by external parties.

Araxxe is committed to maintaining the security of our systems, products, and services. We recognize the valuable role that security researchers and the broader community play in helping us identify and address vulnerabilities.

This Responsible Vulnerability Disclosure Policy outlines our guidelines for reporting security vulnerabilities in our systems. We encourage responsible disclosure and will work with security researchers to validate, remediate, and publicly disclose vulnerabilities in a coordinated manner.

2. History

Version	Date	Author	Descritpion
1.0	2026-03-03	P. Favier	Initial version
1.1	2026-04-13	P. Favier	Fixed typo

3. Scope

This policy applies to:

- All Araxxe websites, applications, APIs, and digital services.
- Third-party services integrated with our systems (if applicable).
- Hardware, firmware, or software products developed by Araxxe.

4. Guidelines and Rules of Engagement

We consider security research conducted under this policy to be:

- Authorized in accordance with applicable laws.
- Exempt from prosecution under the French Penal Code (Articles 323-1).
- Exempt from restrictions in our Terms of Service or Acceptable Use Policy that would otherwise prohibit such testing.

If you are a security expert and want to participate in the security analysis of the Araxxe platform, you must follow the following rules of engagement:

- You must comply with this policy.
- You must not exploit any vulnerability beyond what is necessary to demonstrate its existence.
- You must not disclose vulnerabilities publicly before we have had a reasonable opportunity to remediate them.
- You must not engage in any activity that could harm our users, systems, or data.

The following activities are strictly prohibited:

- Social engineering attacks (e.g., phishing, vishing).
- Physical security vulnerabilities (unless explicitly permitted).
- Denial-of-Service (DoS/DDoS) attacks.
- Spam or unsolicited bulk communications.
- Vulnerabilities in third-party services not under our direct control (unless they impact our systems).

5. Reporting a Vulnerability

If you discover a security vulnerability, we encourage you to report it to us as soon as possible.

How to Report:

- Email: security@araxxe.com
- Encryption: If possible, encrypt your report using our PGP key to protect sensitive information.

What to Include in Your Report:

- A detailed description of the vulnerability.
- Steps to reproduce the issue (proof of concept).
- The affected system(s) or product(s).
- Your contact information (optional but helpful for follow-up).
- Any additional supporting materials (screenshots, logs, etc.).

6. Our Commitment

Upon receiving a vulnerability report, Araxxe commits to:

- Acknowledge receipt of your report within 5 business days.
- Validate the vulnerability and assess its impact.
- Keep you informed of our progress in remediating the issue.
- Work with you to verify the fix (if needed).
- Publicly acknowledge your contribution (if desired) once the vulnerability is resolved.

7. Disclosure Timeline

We aim to resolve critical vulnerabilities within 7 days of confirmation. However, the timeline may vary depending on the complexity of the issue.

- Critical Vulnerabilities (CVSS 9.0-10.0): Target resolution within 7 days.
- High Vulnerabilities (CVSS 7.0-8.9): Target resolution within 14 days.
- Medium/Low Vulnerabilities (CVSS 0.1-6.9): Target resolution within 30-90 days.

If a vulnerability is actively being exploited, we may accelerate our response.

8. Public Disclosure

We believe in coordinated disclosure and will work with you to determine an appropriate timeline for public disclosure. We ask that you:

- Do not disclose the vulnerability publicly until we have confirmed remediation.
- Allow us a reasonable timeframe to fix the issue before any public discussion.

9. Legal Protections

We will not pursue legal action against security researchers who:

- Follow this policy.
- Act in good faith.
- Do not cause harm to our users, systems, or data.

However, we reserve the right to take legal action if:

- The vulnerability is exploited maliciously.
- Sensitive data is accessed, modified, or exfiltrated.
- The report is used for extortion or blackmail.

10. Recognition

We appreciate the efforts of security researchers who help us improve our security. While we do not offer monetary rewards (unless we have a Bug Bounty Program), we may:

- Publicly acknowledge your contribution (with your permission).
- Provide a letter of appreciation.
- List your name in our Security Hall of Fame (if applicable).

11. Contact Information

For questions about this policy, please contact:

- Security Team
- security@araxxe.com

END OF DOCUMENT