AUDITORIA

AUDITORIA.AI

Responsible Disclosure Policy

Effective date: September 1, 2026 | Version 1.0 | Owner: Security & Compliance Team

Our Commitment

Auditoria.ai ("Auditoria," "we," "our," or "us") builds AI agents that finance and audit teams trust with sensitive financial data. Keeping that data and our systems secure is core to our mission, and we know that independent security researchers play an important role in helping us do that.

This Responsible Disclosure Policy explains how to report a security vulnerability you believe you've found in an Auditoria system, what we ask of you while you do, and what you can expect from us in return — including our commitment not to pursue legal action against researchers who follow this policy in good faith.

Scope

This policy applies to security vulnerabilities in systems that Auditoria owns and operates. It does not extend to third-party services we integrate with, or to systems owned by our customers or partners, even if they are used to access Auditoria products.

In scope

- **Production domains and applications —** including auditoria.ai, its subdomains, and Auditoria's customer-facing web applications.
- **APIs —** public and authenticated Auditoria APIs used by our products and integrations.
- **Underlying cloud infrastructure —** that Auditoria directly configures and controls (e.g., misconfigured storage, exposed credentials, authentication bypass).

Out of scope

- **Third-party services and integrations —** including vulnerabilities in vendors, subprocessors, or partner platforms Auditoria relies on. Please report these directly to the vendor; we're happy to help you find the right contact.
- **Customer- or partner-owned systems —** including customer tenants, on-premise deployments, or configurations controlled by the customer rather than Auditoria.
- **Non-technical or social vulnerabilities —** such as social engineering, phishing, or physical attempts to access Auditoria offices, employees, or equipment.
- **Denial of service —** any testing intended to degrade or disrupt the availability of Auditoria services.
- **Findings that require unlikely user interaction, self-XSS, or issues with no demonstrable security impact —** clickjacking on pages without sensitive actions, missing security headers without a working exploit, software version disclosure, and similar low-impact issues are typically not actionable; we ask that you still let us know, but they may not receive an individual response.

Guidelines for Researchers

We ask that you act in good faith and avoid privacy violations, degradation of service, and destruction of data while researching a potential issue. Specifically, please:

AUDITORIA

- Only interact with accounts, data, and systems you own, or for which you have explicit permission from the account holder.
- Avoid automated, high-volume scanning that could degrade service for other users; favor targeted, manual testing.
- Never attempt to access, download, modify, or delete data that does not belong to you — if you encounter customer or personal data during testing, stop immediately, do not copy or retain it, and report it to us right away.
- Do not use denial-of-service, social engineering, or physical-access techniques.
- Give us a reasonable amount of time to investigate and remediate an issue before disclosing it publicly (see "Coordinated Disclosure" below).
- Report only through the channel described in this policy — not through public forums, social media, or ticket systems — until we've had a chance to address it.

How to Report a Vulnerability

Send a report to:

security@auditoria.ai

If your report involves sensitive data, you're welcome to ask us for a PGP key before sending details, or to send a first message describing the issue at a high level so we can arrange a secure channel.

What to include

A clear, well-documented report helps us triage and fix issues faster. Please include:

- A description of the vulnerability and its potential impact.
- The affected system, URL, endpoint, or component.
- Step-by-step reproduction instructions, including any proof-of-concept code, screenshots, or request/response captures needed to reproduce the issue.
- The account, browser, or environment details relevant to reproduction.
- Whether you believe the issue is being actively exploited, or found any indication of prior exploitation.

Please submit one vulnerability per report, unless you need to chain multiple issues together to demonstrate impact.

What You Can Expect From Us

We commit to the following response targets for reports submitted through the channel above:

Milestone	Target
Acknowledgment of receipt	Within 2 business days
Initial triage and severity assessment	Within 5 business days
Status updates while a valid issue is open	At least every 10 business days
Remediation of confirmed critical/high-severity issues	Prioritized; timeline shared with the reporter once triaged

We'll keep you informed as we investigate, let you know once a fix is deployed, and — with your permission — credit you publicly for the finding.

AUDITORIA

Safe Harbor

Auditoria considers security research conducted consistent with this policy to be authorized activity. Specifically, we commit that:

- We will not pursue civil or criminal legal action, or report you to law enforcement, for research conducted in good faith and in accordance with this policy.
- We will work with you to understand and resolve the issue quickly.
- If a third party initiates legal action against you for activity conducted in compliance with this policy, we will make clear that your actions were authorized.

This authorization does not extend to testing of third-party systems, or to activity outside the scope and guidelines described in this policy. If you're ever unsure whether an activity is consistent with this policy, please ask us at security@auditoria.ai before proceeding.

Coordinated Disclosure

We ask researchers not to publicly disclose a vulnerability, or share it with third parties, until we have confirmed it is resolved or otherwise agreed on a disclosure timeline with you. In most cases, we aim to remediate confirmed issues within 90 days of a validated report; if resolution takes longer, we'll explain why and work with you on a mutually agreeable disclosure date.

Recognition

This is a disclosure-only program: we do not currently offer monetary bug bounty rewards. We're genuinely grateful for the work researchers put into responsible disclosure, and where a report leads to a confirmed fix, we're happy to publicly acknowledge the researcher (with their permission) and to provide a reference letter on request.

Questions

For anything not covered here, or to ask before you start testing, contact us at **security@auditoria.ai**.