Responsible Disclosure Policy

Ironmark Authoring Suite — Security Vulnerability Reporting

Effective: March 19, 2026

Safe Harbor

Ironmark will not pursue legal action against any individual or organization that discovers and reports a security vulnerability in good faith in accordance with this policy. We consider responsible security research a service to our customers and to the community, and we commit to working with researchers transparently and without retaliation.

Purpose

Ironmark Authoring Suite is deployed on defense and government networks. Security matters. This policy exists to give anyone who finds a security vulnerability a clear, safe path to report it — and to commit to how we will respond.

This is not a public bug bounty program. We do not advertise it or invite open submissions from the general public. It exists for customers, evaluators, security assessors, and researchers who encounter a potential vulnerability in the course of legitimate work with Ironmark.

How to Report

Email: [security@ironmark-authoring.com]

Please include:

- A description of the vulnerability and where it exists in the product
- Steps to reproduce — enough detail that we can confirm and triage the issue
- The potential impact as you understand it
- Your name and organization (optional but appreciated)

Encrypted submission is welcome. PGP key available on request.

Do not report security vulnerabilities through GitHub issues, support tickets, or any public channel.

What We Commit To

- Acknowledgment of your report within 2 business days
- An initial triage assessment within 5 business days
- Regular status updates while the issue is being addressed
- Notification when the vulnerability has been fixed
- Recognition in our security acknowledgments if you want it — or full confidentiality if you prefer

Response Timelines

We will work to address confirmed vulnerabilities within the following target timelines from the date of confirmation:

Severity	Description	Fix Target
Critical	Authentication bypass, remote code execution, data exposure across customer boundaries	**7 days**
High	Privilege escalation, significant data leak within a single customer instance, denial of service	**30 days**
Medium	Limited impact, requires specific conditions or elevated access to exploit	**90 days**
Low	Minimal impact, defense-in-depth issues, informational findings	**Best effort**

These are targets. Complex vulnerabilities may take longer. We will communicate status throughout and will not go silent on an open report.

Recognition and Rewards

We appreciate researchers who take the time to report vulnerabilities responsibly. For valid confirmed findings, we offer:

Severity	Reward	Recognition
Critical	3 months free service credit (hosted) or extended maintenance (on-premise)	Named acknowledgment (if desired)
High	1–2 months free service credit or extended maintenance	Named acknowledgment (if desired)
Medium	1 month free service credit or extended maintenance	Named acknowledgment (if desired)
Low	Written acknowledgment	Optional listing

Service credits apply to active hosted subscriptions. For on-premise customers, equivalent value is applied as extended maintenance. Rewards are issued after the vulnerability is confirmed and triaged. Recognition is entirely optional — full confidentiality is respected if preferred.

Scope

In Scope

- Ironmark Authoring Suite application (all versions)
- ironmark-authoring.com and demo.ironmark-authoring.com
- Authentication and session management
- API endpoints and access controls
- File handling and document processing
- XML parsing and validation pipeline

Out of Scope

- Customer data on hosted instances — do not test against production instances you do not own
- Denial of service attacks against shared infrastructure
- Physical security
- Social engineering of Ironmark staff
- Vulnerabilities in third-party software that Ironmark does not control
- Issues that require compromised customer credentials to exploit
- Scanner output without a working proof of concept

> **On hosted instances**
> If you are a hosted customer and discover a potential vulnerability, please report it without attempting to verify it against other customers' data. Your instance is isolated — you should only ever be able to see your own data. If you believe you can see data that is not yours, stop immediately and report it.

Good Faith Guidelines

We ask that researchers:

- Only test against instances you own or have explicit permission to test
- Do not access, modify, or delete customer data beyond what is necessary to demonstrate the vulnerability
- Do not disclose the vulnerability publicly before we have had a reasonable opportunity to address it
- Do not use the vulnerability for any purpose beyond demonstrating its existence

We commit to the same good faith in return — transparent communication, prompt response, and no legal action against researchers acting within these guidelines.

Coordinated Disclosure

We support coordinated disclosure. If you report a vulnerability to us, we ask for a reasonable period to address it before public disclosure. We will work with you to agree on a disclosure timeline.

If we have not resolved a Critical or High severity issue within the target timeframe, we understand that you may need to disclose. Please notify us before doing so and we will work to coordinate the disclosure.

Contact

[security@ironmark-authoring.com]

This policy is reviewed annually and updated as needed. Questions about the policy itself can be sent to the same address.