REV	CHANGE DESCRIPTION	DATE
1.0	Creation from AV-CVD-001. Internal policy elements removed.	02/09/2026

Contents

Purpose

AVIRE welcomes reports of security vulnerabilities affecting our products, firmware, cloud services and websites. We operate a Coordinated Vulnerability Disclosure (CVD) process: if you believe you have found a vulnerability, please tell us first and give us the opportunity to investigate and remediate it before the issue is made public.

Reports made in good faith are welcome from anyone — customers, security researchers, partners, installers and end users alike.

How to contact us

Email our security team at security@avire-global.com, or use the reporting form on our website. Both routes reach the same team.

If your report contains sensitive technical detail, exploit code or customer data, please encrypt it. Our PGP public key is published at security.txt.

What to include in your report

The more detail you can give us, the faster we can triage and reproduce the issue. Where possible, please tell us:

- The affected product, model and firmware or software version.
- A description of the vulnerability and the impact you believe it could have.
- Steps to reproduce the issue, or a proof of concept.
- Any supporting evidence such as logs, configuration details or screenshots.
- How you would like to be contacted, and whether you wish to be credited publicly.

Testing rules

Please do not access, modify or delete data belonging to other people, and do not run tests that could disrupt a live installation, or a product's alarm or emergency communication function, or put building occupants at risk.

Good-faith security research

AVIRE supports good-faith security research. Vulnerabilities discovered and reported in good faith, for the purpose of testing, investigating or correcting a security flaw and without malicious intent, are handled under this policy.

We will not pursue legal action against researchers who act in good faith, comply with this policy (including the testing rules above), avoid privacy violations and service disruption, and do not disclose a vulnerability publicly before a coordinated disclosure has taken place.

How we will respond

- We acknowledge receipt of every report within 1 business day.
- We assess and triage the report, and keep you informed while we investigate.
- Where a fix or mitigation is needed, we work on it and coordinate the disclosure timeline with you.

- If you have consented, we credit you as the reporter in the related security advisory.

Disclosure timing

Once a security update is available, we share and publicly disclose information about the fixed vulnerability, including a description, the affected products, the impact, the severity and remediation information. In duly justified cases, publication may be delayed until users have had the opportunity to apply the update.

Our target coordinated-disclosure window is 90 days from the date of the report, unless active exploitation or a separate agreement with the reporter means an earlier or later date is appropriate. We will coordinate disclosure timing with you as far as possible.

Published advisories are notified to connected-product customers through the AVIRE Hub, and are linked from this page.

Third-party and open-source components

Where a vulnerability concerns a third-party or open-source component integrated into one of our products, we report it to the party that maintains that component, and address and remediate it in our product. We inform users of security updates affecting these dependent components as part of the related advisory.

Data protection

Personal data you provide when reporting a vulnerability is processed in line with our privacy policy. Please do not include personal data relating to third parties in your report, and do not attach live customer data — if your report is highly sensitive, email it to security@avire-global.com encrypted with our PGP key instead.

Contact

For questions about this policy or an advisory, contact security@avire-global.com.