COORDINATED DISCLOSURE · ISO/IEC 29147

Vulnerability disclosure policy

How to report a vulnerability in the websites of REVIEWIT SAS or in the REVIEWIT solution, what we expect from the people who report it, and what we commit to in return.

VERSION
1.0 · November 2026

SCOPE
we-reviewit.com domain · REVIEWIT SaaS solution

DISTRIBUTION
Public

CONTENTS

01 Scope
02 How to report a vulnerability
03 What we expect from you
04 Our commitments and timeframes
05 Coordinated disclosure and customer information
06 Good-faith commitment

PURPOSE

The security of the REVIEWIT solution and of the data our customers entrust to us is our priority. If you believe you have found a vulnerability, we want to hear it from you, fix it quickly and keep you informed. This policy draws on the practices of ISO/IEC 29147 (vulnerability disclosure). The timeframes it gives are those of our internal vulnerability management procedure. This is a translation: the French version prevails.

SECTION 01 Scope

IN SCOPE

- The **we-reviewit.com** domain and its subdomains operated by REVIEWIT SAS: public website, Trust Center, consoles and application programming interfaces (APIs) of the solution.
- The REVIEWIT SaaS solution, in all its hosting regions, including the RITA assistant and the collection connectors.

OUT OF SCOPE

- Third-party services, even when used by REVIEWIT or connected to the solution (a customer's identity provider, REVIEWIT's providers): report them to their vendor.
- The data and subscriptions of other customers or of anyone other than you.
- Denial of service, load testing, social engineering, phishing and any physical intrusion.

- Findings with no demonstrated security impact: raw output of an automated tool, displayed software version, missing informational header with no exploitation scenario.

SECTION 02 How to report a vulnerability

Write to **security@we-reviewit.com**, in French or in English. To help us assess your report quickly, please include where possible:

- the website, console or API concerned, with the exact address or endpoint;
- the nature of the vulnerability and its possible impact;
- the steps to reproduce it, with a minimal proof of concept;
- the date of your discovery and how to contact you.

Do not attach any personal data or any customer data you may have seen: describe it without copying it. The information you send us, including your contact details, is used only to handle your report and is not shared with anyone without your consent, unless required by law (questions about your data: **dpo@we-reviewit.com**).

SECTION 03 What we expect from you

- Act in good faith and stay within the scope of section 01.
- Use only your own accounts or test accounts, and access only what is strictly needed to demonstrate the vulnerability; stop as soon as it is demonstrated.
- Do not view, modify, delete or extract any data that does not belong to you. If you access such data by accident, stop, let us know and delete anything you may have kept.
- Do not degrade the service: no denial of service, no mass sending of requests, forms or messages, no malware, no persistent access and no pivoting to other systems.
- Report the vulnerability to us without delay and do not disclose it to third parties before it is fixed and before agreeing on it with us (section 05).
- Do not ask for anything in return for your report or your silence.

SECTION 04 Our commitments and timeframes

Remediation timeframes run from triage, that is, from our assessment of the severity and exploitability of the vulnerability in our context. Severity follows the CVSS score of the advisory or of our own assessment.

STEP	COMMITMENT
Mailbox monitoring	The **security@we-reviewit.com** mailbox is checked every day, 7 days a week.
Acknowledgement	No later than two business days after receipt of the report.
Triage	No later than two business days after receipt of the report. We tell you whether the report is accepted.
Critical vulnerability	CVSS 9.0 or higher, or known active exploitation whatever the score: fix or mitigation within 14 days.

STEP	COMMITMENT
High vulnerability	CVSS 7.0 to 8.9: fix or mitigation within 30 days.
Medium vulnerability	CVSS 4.0 to 6.9: fix within 90 days.
Low vulnerability	Fix in the next planned release.
Closure	The fix is verified by a new scan; we let you know when it is in production.

Every accepted report is entered in our vulnerability register and tracked until closure. We never publish the details of a vulnerability that has not been fixed.

SECTION 05 Coordinated disclosure and customer information

- Once the vulnerability is fixed, you may publish your work on a date agreed with us, without customer data or details that would allow an attack on an unpatched installation.
- Our customers are informed according to our contractual commitments. When an exploited vulnerability leads to a personal data breach, the breach is notified to the customers concerned no later than 24 hours after we become aware of it.
- When an exploitable vulnerability cannot be fixed within the timeframe, the customers concerned are informed, together with the mitigation measures applied.

SECTION 06 Good-faith commitment

REVIEWIT SAS will not take legal action or file a complaint against anyone who has carried out research in good faith in accordance with this policy and has reported the results to us without delay. This commitment binds REVIEWIT SAS only; it does not bind its customers or its providers.

You may also report a vulnerability to the French national cybersecurity agency (ANSSI), under Article L. 2321-4 of the French Defence Code.

No bounty programme. REVIEWIT SAS has no bug bounty programme and pays no reward for a report.

REVIEWIT SAS · Security: **security@we-reviewit.com** · Data protection officer: **dpo@we-reviewit.com**.
Policy reviewed at least once a year. Version 1.0 · November 2026 · the French version prevails.