ZeeDo Security Disclosure Policy

ZeeDo

Version 1 · Zuletzt aktualisiert am 30. Oktober 2026 · Fingerabdruck b7214ea81a60

Rechtstexte werden auf Englisch veröffentlicht; maßgeblich ist der englische Text. Diese Version bleibt unverändert erhalten. Alle Versionen, jeweils mit PDF: https://zeedo.cloud/de/legal/versions/security

1. Our commitment

ZeeDo GmbH ("ZeeDo", "we") wants to hear about security weaknesses in ZeeDo's service. If you find one, please tell us. We will work with you to understand and fix it.

2. No reward

ZeeDo does not run a bug-bounty programme. We offer no monetary reward, bounty, tier, or credit with a payout of any kind for reports. Findings are welcome, are acknowledged within five business days, and are not rewarded. We test our own security, as Annex 2 of our Data Processing Addendum describes under Testing.

3. How to report

3.1 Email **security@zeedo.cloud.** We do not publish an encryption key at launch.

3.2 Please include:

- what you found and where (URL, API endpoint or product area);
- the steps to reproduce it;
- the impact you believe it has; and
- how to contact you.

3.3 Please report as soon as you can, and send one finding per email.

4. What happens next

Step	Our commitment
Acknowledgement	Within 5 **business days** of receiving your report
Assessment	We confirm whether we can reproduce it and how severe we think it is
Fix or plan	Within 30 **days** of the report, we fix the issue or send you a dated plan
Record	We log every report, valid or not, and keep that record for 400 days
Regression test	Each valid finding becomes a permanent case in our automated test suite before we close it

Step	Our commitment
Disclosure	We agree with you when and what to publish. Unless we agree otherwise, you may publish 90 days after your report, or when the fix ships, whichever is earlier

5. Scope

5.1 **In scope:**

- the ZeeDo web application at `zeedo.cloud` and its subdomains;
- the public API at `api.zeedo.cloud/v1`;
- the isolation between one customer's workspace and another's;
- the credential vault, the approval gates, the policy engine and the egress broker;
- ZeeDo's `security.txt`, and any endpoint ZeeDo publishes to identify its bots or to verify their signatures.

5.2 **Reports we especially want:** any way to read or change another customer's data; any way for a bot to leave its machine; any way for a bot to read a stored credential; any way for a bot to carry out a gated action without approval, or to pay, submit a regulated filing or defeat a human-verification challenge; any way to forge or replay an approval.

5.3 **Prompt injection.** Prompt injection is unsolved industry-wide. A report that a bot can be persuaded by text in a web page or email is useful, but on its own it is expected behaviour. It becomes a vulnerability when it lets the bot do something irreversible without a human, or reach data or credentials it should not.

5.4 **Out of scope:**

- websites and services ZeeDo bots visit or connect to, which belong to third parties;
- other customers' workspaces, data or accounts;
- social engineering of ZeeDo staff or customers;
- physical attacks on offices or data centres;
- denial-of-service or volume testing;
- the infrastructure and services of our hosting providers and vendors (for example Scaleway, OVH, Amazon Web Services, Neon, Temporal Cloud and Vercel).

6. Rules for testing

6.1 Test only against accounts you created. A Free account is enough for most testing.

6.2 Do not access, change, keep or delete data that is not yours. If you reach another customer's data by accident, stop, do not copy it, and tell us at once.

6.3 Do not degrade the service for others. Stay within the Acceptable Use Policy, including fair use and per-website rate limits.

6.4 Do not use a ZeeDo bot to test or attack third-party websites.

6.5 Do not publish or share the details of a finding before the time section 4 allows.

6.6 Do not demand payment. We do not pay for findings (section 2).

7. Safe harbour

7.1 EU variant

If you research and report in good faith and follow this policy:

- we consider your research authorised by ZeeDo for the purposes of our own systems;
- we will not bring civil claims against you in relation to that research;
- we will not report that research to the police or a prosecutor as a criminal offence, and will not make a request for prosecution (Strafantrag) in relation to it;
- we will not treat your research as a breach of our Terms of Service or Acceptable Use Policy; and
- if a third party takes action against you for research that complied with this policy, we will make clear that your activity was authorised by us.

This safe harbour covers only ZeeDo's own systems and ZeeDo's own rights. It cannot authorise access to third-party systems or to data that belongs to others, and it cannot bind public prosecutors or courts.

7.2 US variant

If you research and report in good faith and follow this policy, we consider your research authorised under the Computer Fraud and Abuse Act and similar state laws, we waive our own claims under the anti-circumvention provisions of the DMCA for circumvention of our own technical measures that the research required, and we will not bring a lawsuit against you for it.

8. Acknowledgement

We do not publish a list of researchers at launch. If we ever name a researcher, it will be only with their permission, it will not be described as a reward, and it will not use a leaderboard, points or tiers.

9. Contact

security@zeedo.cloud