aginion

Vulnerability Disclosure Policy

Aginion Luxembourg

Date: 2024-02-19

Classification: Public

Purpose

Aginion Luxembourg ("we") takes the security of our systems, and of the data our customers entrust to us, seriously. This policy explains how to report a security vulnerability you have found in our systems, what you can expect from us in return, and the conditions under which we authorise good-faith security research. Our aim is to give researchers, customers, and members of the public a clear and safe route to report weaknesses so that we can fix them before they are exploited.

This policy covers our own infrastructure only. It does not authorise testing of any system we operate on behalf of a customer — see Scope.

Scope

In scope — internet-facing systems and services that we own and operate, including:

- our public website and the AI assistants hosted on it;
- our customer and service-desk / ticketing portals;
- our email, DNS, and public API endpoints;
- our corporate cloud tenants and remote-management infrastructure;
- aginion.com, aginion.de, aginion.lu, aginion.net and their subdomains

Reports of weaknesses in the AI systems we operate — for example prompt injection, unintended disclosure of data, or bypass of a safety control in our chatbots — are explicitly welcome and in scope.

Out of scope:

- Customer environments and any systems we manage on a customer's behalf. We can only authorise testing of assets we own; only the customer, as owner, can authorise testing of their systems. Do not probe, access, or test any customer system, even where you can tell that we manage it. If you become aware of an issue in a customer environment without testing it, you may still notify us and we will route it appropriately.
- Third-party services and platforms we use but do not control (report those to the relevant provider).
- The findings listed under "Findings we generally do not accept" below.

How to report

Send your report to security@aginion.com. For sensitive details, please encrypt your message using our PGP key, available at https://aginion.com/.well-known/pgp-key.txt

A useful report includes the affected system or URL, a description of the vulnerability and its potential impact, and clear, reproducible steps or a proof of concept. Please send one report per vulnerability.

Safe harbour

We consider security research and disclosure carried out in good faith and in accordance with this policy to be authorised. For such activity, we will not initiate or support legal action against you, and we will not report you to law enforcement. If a third party brings legal action against you for activity conducted in line with this policy, we will take steps to make known that your actions were authorised by us.

This authorisation extends only to our own in-scope systems. It does not permit you to access, disrupt, or damage any customer system or third-party service, and it does not waive any rights of our customers or of third parties. If you are unsure whether a system is in scope, ask us before you test it.

What you can expect from us

- We will acknowledge receipt of your report within 3 business days.
- We will provide an initial assessment within 10 business days and tell you whether we consider the report valid.
- We will keep you informed of our progress at reasonable intervals until the issue is resolved.
- We will coordinate the timing of any public disclosure with you (see below).

What we ask of you

- Act in good faith and stay within the scope of this policy.
- Access only the minimum data necessary to demonstrate the vulnerability. Do not view, copy, modify, delete, or remove data beyond what is required to prove the issue.
- Do not degrade or interrupt our services — no denial-of-service testing, high-volume automated scanning, or spam.
- Do not use social engineering against our staff or customers, and do not attempt physical access to our premises.
- Keep the details of any vulnerability confidential until we have had a reasonable opportunity to remediate it.
- Do not demand payment in return for withholding disclosure; such demands will be treated as extortion, not research.

Coordinated disclosure

We support coordinated disclosure. We ask that you give us a reasonable period — by default 30 days from our acknowledgement — to remediate a valid vulnerability before publishing any details, and that you coordinate the timing and content of any publication with us. For complex issues we may agree a longer period. We are glad for you to publish once the issue is resolved or the agreed period has elapsed.

Recognition

With your consent, we are happy to credit researchers who report valid vulnerabilities. This is a disclosure policy, not a paid bug-bounty programme; we do not currently offer financial rewards.

Findings we generally do not accept

On their own, and without a demonstrated, exploitable impact, the following are typically out of scope: output from automated scanners; missing security headers or cookie flags; SPF, DKIM, or DMARC configuration suggestions; self-XSS; clickjacking on pages with no sensitive action; rate-limiting observations; software version disclosure; and general best-practice recommendations that do not correspond to a specific vulnerability.

Relationship to our other policies

A confirmed vulnerability report may be handled as a security incident under our Incident Response Policy. This policy complements our routine security testing, including independent penetration testing, by providing a channel for issues found outside that testing.

Governance and review

This policy is reviewed at least annually and updated as needed.

- End of Document -

aginion

Aginion Group

Legally represented by:

Aginion Luxembourg

142 Boulevard de la Pétrusse
L-2330 Luxembourg
R.C.S. Luxembourg B184509

This document is provided by:

Aginion Infosec

Tel: +352 2740 5949
E-Mail: security@aginion.com