Defensio SECaaS — Vulnerability Assessment & Scanning Authorization Agreement

Version 1.1 · in force from 25 July 2026 · supersedes v1.0 Provider: **Fidem S.r.l.**, Via Don G. B. Tessari 14/A, 37030 Lavagno (VR), Italy — VAT IT04438280234. Accepted at signup; acceptance is recorded with version, content hash, IP, user-agent and timestamp.

1. Purpose

Defensio SECaaS performs **active security testing** — exposure/port scanning, web-application scanning (DAST), vulnerability scanning, and data-leak monitoring — against targets you designate. Active testing of systems you are not authorised to test is unlawful in most jurisdictions. This Agreement is how you provide, and warrant, that authorisation.

2. Your authorisation and warranty

You represent, warrant and agree, on a continuing basis, that: 1. You **own, or are expressly authorised by the owner to security-test**, every target (domain, subdomain, IP or asset) you register. 2. You hold all internal and third-party approvals needed to authorise active scanning and breach monitoring of those targets. 3. For **data-leak monitoring**, you are entitled to monitor each email address you enter and have made any notices or obtained any consents required in respect of the individuals concerned; **you act as data controller** for those addresses and Fidem acts as your **processor**. 4. You will not use the platform against any system, network or address you are not authorised for, nor for any unlawful purpose.

3. Scope and method

- Testing is **non-destructive by design** but is active: it sends real traffic, may be detected by the target's defences, and may briefly affect target performance. You accept this for authorised targets.
- Fidem scans only the targets you register, with the engines you enable, on your configured schedule.
- Fidem does **not** exploit vulnerabilities, pivot, exfiltrate data, establish persistence, or conduct social engineering. Findings are reported, not weaponised.

4. Your obligations

- Keep authorisation current and **remove any target** you cease to be authorised for.
- Do not register third-party systems, competitor assets, or addresses you may not monitor.
- **Retain documented proof of authorisation** for every target — including, for assets on shared or cloud infrastructure, any provider authorisation required under that provider's penetration-testing policy — and produce it to Fidem on reasonable request.
- Maintain your own backups. Active testing carries inherent, if low, risk.

5. Indemnity and liability

You will indemnify and hold Fidem harmless against third-party claims, losses, fines and reasonable legal costs arising from your breach of the warranty in §2 — that is, from testing or monitoring you were not entitled to authorise. Fidem's liability is limited as set out in the Terms of Service. Fidem is not liable for consequences of testing you authorised (for example a target's own instability while under scan).

6. Suspension

Fidem may suspend, refuse or remove any target or monitored address it reasonably believes is unauthorised, abusive or unlawful, and may disarm scanning on suspension or non-payment.

7. Evidence

Acceptance is recorded in Fidem's consent register (document version, content hash, IP address, user-agent, timestamp). Scanning is additionally gated on a verified email identity and an active subscription.

8. Governing law

Governed by the laws of **Italy**; exclusive venue the **courts of Verona**. The service is offered to **EU customers only** at launch. If non-EU customers are supported in future, they additionally accept that the authorisation must be lawful in their own and the target's jurisdiction (for example the US Computer Fraud and Abuse Act or the UK Computer Misuse Act).