Responsible Disclosure Program

Bug Bounty & Security — Aureus IA SPRL

1. Scope

In scope: app.aureussocial.be (main application), REST API v1.

Out of scope: aureusia.com (corporate site), DDoS attacks, social engineering, third-party vulnerabilities without PoC.

2. Rewards

Severity	Type	Reward
Critical	RCE, SQLi, full DB access, auth bypass	EUR 500-2,000
High	IDOR on NISS/salary data, stored XSS, SSRF	EUR 200-500
Medium	CSRF on critical actions, information disclosure	EUR 50-200
Low	Reflected XSS, missing headers, open redirect	Hall of Fame

3. Rules of Engagement

1. Do not access, modify or delete other users' data.
2. Do not exfiltrate personal data (NISS, salaries, IBAN).
3. Do not perform destructive attacks or denial of service.
4. Do not test in production without prior agreement.
5. Report via security@aureusia.com with description, PoC and impact.

4. Process

1. Receipt: Acknowledgment within 48 hours.
2. Triage: Severity assessment within 5 business days.
3. Fix: Patch by severity (critical: 24h, high: 7d, medium: 30d).
4. Reward: Payment after fix validation.
5. Disclosure: Coordinated publication after 90 days or after fix.

5. Safe Harbor

Researchers who follow these rules will not face legal action. We commit to not initiating legal proceedings against researchers acting in good faith.

6. Contact

Email: security@aureusia.com — Languages: FR, NL, EN, DE