AIO Responsible Disclosure Policy

[Last Updated: 15 October 2025]

1. Purpose

At AIO Technology EOOD ("AIO," "we," "our," or "us"), security is at the core of everything we do. We value the contributions of security researchers and ethical hackers who help us protect our users and infrastructure.

This Responsible Disclosure Policy outlines how to report potential security vulnerabilities in a safe, responsible, and coordinated manner — and how we commit to handling such reports.

2. Scope

This policy applies to all digital assets owned, operated, or managed by AIO, including:

- https://aio.cash and related subdomains
- API endpoints (api.aio.cash, dashboard.aio.cash)
- AIO Wallet and Blockchain Payment Gateway interfaces
- Any connected web or mobile applications developed by AIO

3. Principles of Responsible Disclosure

We ask researchers to:

1. Act in good faith and report vulnerabilities responsibly.
2. Avoid privacy violations, data leaks, or service disruptions
3. Give AIO reasonable time to investigate and fix the issue before public disclosure (minimum 90 days).
4. Never exploit a vulnerability beyond the extent necessary to prove its existence.
5. Do not access, modify, or delete data that does not belong to you.

6. Do not perform DoS/DDoS attacks or use automated scanning tools that could affect system availability.

4. How to Report a Vulnerability

You can report potential vulnerabilities via encrypted email to our security team:

Email: security@aio.cash
PGP Key Fingerprint: F23A 6C92 17F0 4A7B 9D1C 72B9 2D1F 8BE7 65AA 9C42
Download Public Key: https://aio.cash/pgp.txt

Please include:

- A detailed description of the vulnerability (with steps to reproduce)
- The affected domain, endpoint, or API function
- Screenshots or proof of concept (if applicable)
- Your contact information (for acknowledgment and coordination)

5. Acknowledgment & Response (SLAs)

Stage	Description	SLA / Time Frame	Responsible Party

1. Receipt | Report submitted via encrypted email | Within 1 business day | Security Team
2. Acknowledgment | Confirmation email sent to reporter | Within 3 business days | Security Team
3. Assessment | Verify validity and severity | Within 7 business days | Security & Engineering
4. Remediation | Fix developed, tested, and deployed | Within 30 days (critical) / 60 days (medium) | DevOps / Engineering
5. Disclosure Coordination | Public disclosure after remediation or 90 days | Case-dependent | AIO & Reporter

6. Recognition

AIO appreciates responsible disclosure and may recognize researchers publicly on our Security Hall of Fame page (with consent). While AIO does not currently offer a financial bounty, non-financial recognition or private acknowledgment may be provided for significant findings.

7. No Legal Action Guarantee

AIO pledges not to pursue or support legal action against researchers who act in good faith under this policy and avoid causing harm, data loss, or disruption.

8. Data Protection & Confidentiality

All vulnerability reports and related data are treated as confidential security information, protected under GDPR Article 32, the EU NIS2 Directive (2023), and AIO's internal Information Security Policy.

9. Contact Information

AIO Technology EOOD
Vitosha Blvd №4, 1st Floor, 1000 Sofia, Bulgaria
Email: security@aio.cash
Website: https://aio.cash/security

10. Policy Review

This policy is reviewed annually or after significant infrastructure or regulatory changes. The "Last Updated" date reflects the latest approved version.