ELYRA

AUTONOMOUS INTELLIGENCE NETWORK

NETWORK INITIALIZED

Security Policy & Responsible Disclosure

How to report a vulnerability, what to expect from us, and what Safe Harbor means for you.

DOCUMENT	VERSION	COMPANION TO	PHASE
SECURITY POLICY	**0.1**	**WHITEPAPER**	**GENESIS TESTNET**

Elyra is an experimental protocol under active development. This document may evolve as research and development progress and does not constitute financial, legal or investment advice.

Security Policy

Responsible disclosure guidelines for security researchers.

Elyra takes security seriously and welcomes reports from independent security researchers. This document explains how to report a vulnerability responsibly, what to expect from us in return, and what is in and out of scope.

BEFORE YOU CONTINUE

If you have already exploited a vulnerability beyond what is necessary to demonstrate it, or accessed data that isn't yours, please read Section 3 carefully — it directly affects whether Safe Harbor protection applies to your report.

1. Scope

In Scope

- Elyra Genesis Testnet infrastructure
- Published smart contracts (testnet and, later, the ELY token contract)
- Official RPC endpoint
- Official block explorer
- Official faucet
- elyrachain.com and official subdomains

Out of Scope

- Third-party wallets (MetaMask, Rabby, etc.)
- Third-party infrastructure providers
- Social engineering against team members or the community
- Denial-of-service testing against shared/public infrastructure
- Spam, UI/UX suggestions, or missing security headers with no demonstrable impact

2. How to Report

Email **security@elyrachain.com** with:

- A clear description of the vulnerability and its potential impact
- Step-by-step reproduction instructions
- Any proof-of-concept code, transaction hashes, or screenshots
- Your contact details and, if relevant, a wallet address for potential reward payment

ENCRYPT SENSITIVE REPORTS

If your finding is severe (e.g. a fund-draining vulnerability), consider requesting a PGP key from the security contact before sending full details over email.

3. Responsible Disclosure Guidelines

To qualify for Safe Harbor protection (Section 5), you must:

- Give us a reasonable time to investigate and fix the issue before any public disclosure (minimum 90 days, unless otherwise agreed)
- Make a good-faith effort to avoid privacy violations, data destruction, and service disruption during your testing
- Only interact with accounts, data, and funds that are your own or explicitly provided for testing
- Not exploit a vulnerability beyond the minimum necessary to demonstrate it (e.g. do not drain a vulnerable contract beyond a proof-of-concept amount)
- Not publicly disclose, sell, or share the vulnerability with third parties before a fix is released

NOT QUALIFYING FOR SAFE HARBOR

Reports involving fund theft beyond proof-of-concept amounts, public disclosure before a fix, or attacks against real users will be treated as security incidents rather than responsible disclosures, regardless of intent.

4. What to Expect From Us

STEP	TARGET TIMELINE
Acknowledgment of report	Within 5 business days
Initial severity assessment	Within 10 business days
Status updates	At least every 2 weeks until resolved
Fix or mitigation	Timeline depends on severity and complexity

These are target timelines, not contractual guarantees — Elyra is an early-stage project and response times may vary, particularly during the Genesis Testnet phase.

5. Safe Harbor

GOOD-FAITH RESEARCH IS WELCOME

Elyra will not pursue legal action against researchers who discover and report vulnerabilities in good faith, in accordance with the guidelines in Section 3. This commitment applies regardless of whether a monetary reward is ultimately paid.

6. Rewards

Elyra does not currently operate a fixed bug-bounty fee schedule. Verified, in-scope reports are assessed and rewarded on a case-by-case basis, considering severity, exploitability, and quality of the report. This section will be updated with a formal bounty structure closer to, or following, the third-party audit and token launch referenced in the Whitepaper.

7. Coordinated Disclosure

Once a reported vulnerability is fixed, Elyra may choose to publish a post-mortem or credit the researcher (with their permission). We will always coordinate the timing and content of any public disclosure with the reporting researcher first.