Skuridat Responsible Disclosure Policy

Effective Date: 1 July 2025

Scope of the Disclosure Program

Skuridat's Responsible Disclosure Policy applies to the following systems and services:

- skuridat.com and its subdomains
- Skuridat's threat management platform and supporting infrastructure
- Any publicly accessible IPs or endpoints directly managed by Skuridat

This policy does not extend to third-party platforms, infrastructure not owned or operated by Skuridat, or systems of clients using our services unless explicitly agreed upon.

Physical security vulnerabilities, social engineering, or denial-of-service (DoS) testing are not within scope.

Legal Position and Commitment to Good Faith Research

Skuridat values the role of independent security researchers and ethical hackers in improving cybersecurity. We will not pursue legal action against individuals who:

- Act in good faith and comply with this policy
- Limit testing to systems within the defined scope
- Do not exploit, modify, or delete data during testing
- Avoid service disruption, privacy breaches, or data extraction
- Comply with applicable legislation, including, but not limited to, the EU Directive on Attacks Against Information Systems and Dutch Criminal Code, Article 138ab (Computervredebreuk)

We reserve the right to request clarifications and may involve regulatory bodies (e.g., NCSC-NL, ENISA) for assistance.

How to Submit a Vulnerability Report

To report a vulnerability, please email:

- disclosure@skuridat.com

Initial contact should include:

- A clear and concise description of the vulnerability
- IP addresses, domain names, or endpoints involved
- A proof-of-concept or reproduction steps (if applicable)
- Your contact details or anonymity preference

We may establish a secure communication channel (i.e., PGP) for sensitive exchanges.

- PGP: [...]

Handling, Response, and Credit

Once a report is received:

- We will acknowledge receipt within 5 business days
- We aim to provide a status update within 15 business days

- If validated, we will work toward resolution within 90 days, or as mutually agreed
- Researchers may receive public credit after remediation, unless anonymity is requested

In the event of a disagreement on severity or handling, Skuridat may engage a neutral party such as NCSC-NL for independent guidance.

Preferences and Prioritization

Reports that help us triage more effectively include:

- Technical clarity and reproducibility
- Validated proof-of-concept code
- No reliance on generic automated outputs without context

Submissions solely based on outdated headers, missing SPF records, or general security misconfigurations may be deprioritized.

Final Notes

Skuridat's Responsible Disclosure Program is designed to enhance collaboration between the cybersecurity community and our internal teams. We welcome responsible reports and aim to maintain a fair, safe, and legally secure process for all parties involved.

This document may be updated periodically to reflect changes in scope or legislation.