Vulnerability Disclosure Policy at Klippan Safety

Introduction

This policy describes how external parties can responsibly report potential security vulnerabilities. It is part of Klippan Safety's information security and regulatory compliance efforts.

Scope

This policy applies to digital services, applications, and infrastructures provided by or under the responsibility of Klippan Safety, including internally developed and third-party components. Testing of systems or environments not owned or controlled by Klippan Safety is excluded.

Principles for Responsible Disclosure

Vulnerabilities must be reported responsibly to protect users, data, and services. Reporters must not:

- Impact availability, integrity, or confidentiality
- Access, modify, or interact with data
- Use social engineering, phishing, physical intrusion, or denial-of-service techniques

Reporting Vulnerabilities

Reports should include a description of the vulnerability, reproduction steps, supporting evidence if available, and contact information. Reports should be sent to: security@klippan-safety.se Reporters are expected to treat all discovered information as confidential and not disclose details that could harm our operations.

Our Handling Process

All reports are handled through a structured process:

1. **Acknowledgement** – Receipt is normally acknowledged within five (5) business days.
2. **Assessment** – The security team verifies the vulnerability and assesses its severity.
3. **Remediation** – Appropriate corrective and risk-mitigating actions are initiated.
4. **Reporting to Authorities** – When legally required
5. **Dialogue** – Ongoing communication is maintained as needed.

Liability Disclaimer and Good Faith

If the reporter acts in good faith and follows this policy, we will not take legal action related to the report.

Klippan, 2026-01-15

Gabriel Grelte, CEO