

Bug Bounty Policy

Document Owner: Emil Rasmussen, CTO

ENTERSPEED A/S is committed to maintaining the security and integrity of its systems and data. While there is no formal bug bounty programme in place, ENTERSPEED A/S welcomes responsible disclosures from external security researchers and may, at its discretion, offer recognition for valuable contributions.

This policy applies to any external individual or organization reporting a security vulnerability in ENTERSPEED A/S-owned systems.

Scope

This policy applies to systems and services that are owned and operated by ENTERSPEED A/S and are publicly accessible. Reports must demonstrate a real and reasonable security impact—such as unauthorized access, data exposure, or flaws affecting service integrity.

In scope:

- Public APIs and web applications managed by ENTERSPEED A/S
- Authentication and session management flows
- Server-side logic or access control issues
- Configuration vulnerabilities on infrastructure directly managed by ENTERSPEED A/S

Out of Scope

ENTERSPEED A/S does not accept or reward reports that:

- Result solely from automated scanning or basic reconnaissance techniques
- Involve third-party services or software not managed by ENTERSPEED A/S
- Concern non-exploitable findings such as missing headers, lack of rate limiting, or outdated libraries with no proven impact
- Attempt Denial-of-Service (DoS), brute-force, or spam attacks

- Include phishing, social engineering, or physical intrusion

Reporting Guidelines

To report a vulnerability, researchers must send an email to **security@enterspeed.com** including:

- A clear and concise description of the issue
- Affected endpoints, components, or environments
- Step-by-step instructions to reproduce the issue
- Any relevant proof-of-concept material (e.g. screenshots, logs, or code)

Reports must be submitted in good faith and should not include data accessed without authorization.

Recognition

ENTERSPEED A/S does not guarantee monetary rewards but may offer discretionary recognition or non-monetary tokens of appreciation for impactful, well-documented, and responsibly disclosed vulnerabilities.

Acknowledgment decisions are made based on severity, quality of the report, and the potential impact on systems or data.

Safe Harbor

ENTERSPEED A/S will not pursue legal action against individuals who:

- Engage in testing within the bounds of this policy
- Avoid actions that could negatively impact the availability or integrity of services
- Refrain from accessing or altering data that does not belong to them
- Provide ENTERSPEED A/S with a reasonable time to respond before any public disclosure
- Any testing or reporting activity must be in compliance with applicable laws.

Policy Updates

ENTERSPEED A/S may revise this policy at any time. The version available on the official website should be considered the current policy.

Version	Date	Reviewer	Approver
1.0	2 July 2025	Emil Rasmussen, CTO	Emil Rasmussen, CTO