Vulnerability Disclosure Policy

GRIEG CONNECT AS

Date 01.09.2025
Ver 1.0

1 PURPOSE

1.1 This policy outlines how Grieg Connect handles reports of security vulnerabilities, encourages responsible disclosure, and aims to improve the security and safety of our systems, applications, and infrastructure.

2 SCOPE

2.1 This policy applies to all systems, services, and products operated by Grieg Connect, means it includes "all digital assets" provided, developed and operated by the company.

3 OUR COMMITMENT

3.1 Grieg Connect is committed to working collaboratively with security researchers, and the community to identify, evaluate, and remediate vulnerabilities. We value and appreciate responsible disclosures that help us improve security for our customers, partners, and employees.

4 HOW TO REPORT A VULNERABILITY

4.1 Please send your report via e-mail to:

Support@griegconnect.com

4.2 Include in your report:

- Description of the vulnerability
- Affected systems or assets
- Steps to reproduce (if applicable)
- Any supporting evidence or screenshots
- Contact information for follow-up

5 RESPONSIBLE DISCLOSURE

- Upon receiving a report, we will acknowledge receipt promptly and under normal circumstances within 3 business days.

We ask that you:

- Refrain from publicly disclosing the vulnerability until it has been fixed and our team has communicated the resolution. Provide us with reasonable time to resolve the issue before you disclose it publicly if you must. We request at least 30 days.
- Avoid any malicious activities, including exploiting or damaging systems.
- Use only the approved scope and testing methods.

6 WHAT TO EXPECT

- We will evaluate the report and work towards a remediation plan.
- We will keep you informed on the status and resolution timeline.
- We may request additional information if needed.
- When we have addressed the vulnerability, we will keep you updated on the progress of resolving the issue.

7 LEGAL AND ETHICAL CONSIDERATIONS

- We encourage ethical behavior and responsible disclosure.
- Conducting activities outside the scope or in a malicious manner may be subject to legal action.
- This policy does not grant permission to access or test systems outside the scope of responsible testing or beyond the bounds of the report.

8 TERMS AND CONDITIONS

You confirm to Grieg Connect that:

- You have not exploited or used in any manner, and will not exploit or use in any manner (other than for the purposes of reporting to Grieg Connect), the discovered vulnerabilities and/or errors;
- You have not engaged, and will not engage, in testing/research of systems with the intention of harming Greig Connect, its customers, employees, partners or suppliers;
- You have not used, misused, deleted, altered or destroyed, and will not use, misuse, delete, alter or destroy, any data that you have accessed or may be able to access in relation to the vulnerability and/or error discovered;
- You have not conducted, and will not conduct, social engineering, spamming, phishing, denial-of-service or resource-exhaustion attacks;
- You have not breached, and will not breach, any applicable laws in connection with your report and your interaction with Grieg Connect product or service that lead to your report.
- You agree not to disclose to any third party any information related to your report, the vulnerabilities and/or errors reported, nor the fact that a vulnerabilities and/or errors has been reported to Grieg Connect.
- You agree that you are making your report without any expectation or requirement of reward or other benefit, financial or otherwise, for making such report, appropriate recognition may be provided under condition that regulations given by this policy is followed.

9 OUR COMMITMENT TO YOU

- We will act in good faith and consider your report a commitment to improving overall security.
- We will respect your privacy and keep your identity confidential if desired.

10 CHANGES TO THIS POLICY

Grieg Connect reserves the right to update this policy at any time.

Updates will be posted at https://griegconnect.com