Driverr Technologies Ltd

Vulnerability Disclosure Policy

Version 1 - June 2026 - Driverr Technologies Ltd - Company No. 17184545

Driverr Technologies Ltd takes the security of our platform and the personal data of our drivers seriously. We welcome reports from security researchers, drivers and members of the public who identify potential vulnerabilities in our systems.

1. Scope

This policy applies to the following Driverr systems and services:
The Driverr app at app.driverr.app
The Driverr marketing website at driverr.app
The Driverr waitlist at waitlist.driverr.app
The Driverr API and server-side infrastructure
The Driverr Supabase database and storage

This policy does not apply to third-party services used by Driverr such as Supabase, Stripe, Vercel or Resend. Vulnerabilities in those services should be reported directly to the relevant provider.

2. How to Report a Vulnerability

If you discover a potential security vulnerability in any Driverr system please report it to us as follows:

Email: hello@driverr.app
Subject line: Security Vulnerability Report - [brief description]

Please include as much of the following information as possible in your report:
A description of the vulnerability and the potential impact.
The URL or location in the app where the vulnerability was identified.
Steps to reproduce the vulnerability.
Any proof of concept code or screenshots if applicable.
Your name and contact details if you are happy to be contacted for follow-up.

3. Our Commitments to You

When you report a vulnerability to us in good faith we commit to the following:
We will acknowledge receipt of your report within 5 business days.
We will investigate the report and provide an initial assessment within 14 business days.
We will keep you informed of our progress as we work to resolve the issue.
We will not take legal action against you for reporting a vulnerability in good faith provided you comply with the guidelines in this policy.
We will credit you in our security acknowledgements if you wish to be named and your report results in a confirmed fix.

4. Responsible Disclosure Guidelines

We ask that you follow these guidelines when researching and reporting vulnerabilities:
Do not access, modify or delete data that does not belong to you.

Do not perform actions that could harm the availability of the Driverr service for other users.
Do not disclose the vulnerability publicly until we have had a reasonable opportunity to investigate and resolve it - we ask for a minimum of 90 days from the date of our acknowledgement.
Do not use the vulnerability to access personal data of other drivers beyond what is necessary to demonstrate the vulnerability.
Do not perform social engineering attacks against Driverr staff or drivers.
Do not submit automated vulnerability scanners without prior permission.

5. Out of Scope

The following are outside the scope of this policy and should not be reported:
Vulnerabilities in third-party services not directly controlled by Driverr.
Missing security headers that do not directly enable a security vulnerability.
Clickjacking on pages with no sensitive functionality.
Self-XSS attacks that require the victim to enter malicious code themselves.
Rate limiting on non-critical endpoints.
Reports generated purely by automated scanning tools without manual verification.

6. No Bug Bounty

Driverr Technologies Ltd does not currently operate a paid bug bounty programme. We are a pre-revenue seed stage startup and are unable to offer financial rewards at this stage. We are grateful for all good-faith reports and will acknowledge contributors publicly where permitted.

7. Legal

Driverr Technologies Ltd will not pursue civil or criminal action against security researchers who identify and report vulnerabilities in good faith in accordance with this policy. We consider good-faith security research to be a valuable contribution to the security of our platform and the protection of our drivers' data.

8. Contact

Security vulnerability reports: hello@driverr.app with subject line Security Vulnerability Report.
General security questions: hello@driverr.app

9. Initial Response Template

Use the following template to respond to any email received with the subject line "Security Vulnerability Report". Respond within 24 hours of receipt.

Subject: Re: Security Vulnerability Report - Received

Hi [Name],

Thank you for taking the time to report this to us. We take security seriously and genuinely appreciate responsible disclosure from the community.

We have received your report and will investigate it thoroughly. Here is what happens next:
We will acknowledge your report within 5 business days with an initial assessment.
We will keep you updated throughout our investigation and remediation.
If your report results in a confirmed fix we will credit you in our security acknowledgements if you wish to be named.

Please do not disclose this vulnerability publicly until we have had the opportunity to investigate and resolve it. We ask for a minimum of 90 days from this acknowledgement.

If you have any additional information that may help our investigation please reply to this email.

Thank you again for helping us keep Driverr and our drivers secure.

Jeldon Fernandes
Founder and CEO
Driverr Technologies Ltd
hello@driverr.app
driverr.app