SECURITY POLICY FOR GREENLINK LOGISTICS

Effective Date: 19th February 2026

1. INTRODUCTION
At GreenLink Logistics, the security of your fleet and operational data is our top priority. This Security Policy outlines the technical and organizational measures we take to protect our infrastructure, application, and your data.

2. DATA PROTECTION & ENCRYPTION
- In Transit: All data sent to and from the GreenLink platform is encrypted in transit using industry-standard Transport Layer Security (TLS/HTTPS).
- At Rest: Customer data stored in our PostgreSQL database is encrypted at rest using Amazon Web Services (AWS) RDS encryption standards.
- Passwords: We do not store plain-text passwords. All user passwords are cryptographically hashed and salted using bcrypt before being saved to the database.

3. AUTHENTICATION & ACCESS CONTROL
- JWT Authentication: We utilize stateless JSON Web Tokens (JWT) for secure user sessions. Tokens are signed to prevent tampering.
- Role-Based Access Control (RBAC): The platform strictly enforces access control on the backend. Drivers can only access data pertaining to their specific assigned routes, while Dispatchers have administrative access limited to their specific operational workspace.

4. CLOUD INFRASTRUCTURE
- Hosting: The application is hosted on Amazon Web Services (AWS), utilizing secure EC2 instances and managed RDS databases.
- Containerization: Our frontend, Java Spring Boot backend, and Python optimization engine are containerized using Docker, ensuring isolated execution environments and consistent security boundaries.
- Firewalls: We utilize AWS Security Groups to act as a virtual firewall, blocking unauthorized external traffic and ensuring the database is only accessible by the application backend.

5. VULNERABILITY REPORTING
We believe that working with the security community is crucial to keeping our users safe. If you believe you have discovered a security vulnerability in GreenLink Logistics, please do not disclose it publicly.

Report it to us immediately at *jamidararnav@gmail.com*. We will investigate all legitimate reports and work to resolve the issue promptly.