Security Overview

Last updated 25 July 2026

This overview describes the technical and organisational measures that protect the ALGOZ OPS platform and the data it holds. It supports the Privacy Policy and Annex II of the Data Processing Agreement.

Architecture

ALGOZ OPS is a multi tenant application built on Google Firebase and Google Cloud Platform. Each Customer company is a separate tenant. The web consoles and the installable and Android apps talk to managed Google Cloud services for authentication, database, file storage and serverless functions.

Encryption

All traffic to and from the platform is encrypted with HTTPS/TLS. HTTP Strict Transport Security is enforced. Data at rest in Google Cloud is encrypted using the provider’s managed encryption.

Authentication and access control

Users authenticate through Firebase Authentication. Access is governed by role based permissions and signed identity claims that record a user’s company, role and rank. Administrative capabilities are separated from ordinary use, and company owner functions are further restricted. Expired or suspended company subscriptions block access for the whole company.

Tenant isolation

Data is separated per company and enforced on the server by security rules that check each request against the signed claims of the requesting user. A user cannot read or write another company’s data. Sensitive company secrets, such as a messaging bot token, are stored server side and never sent to user devices.

Application safety features

The platform includes operational safety controls: rotating QR agent identification that cannot be reused from a screenshot, a duress PIN, welfare check ins, geofence and rally alerts, and an audit trail of key actions across operations.

Data hosting, backups and recovery

Customer data is stored in Google Cloud. The database supports point in time recovery and scheduled backups. Server side upload folders are additionally backed up. Deletion on the platform removes data from the live service, and backup copies are purged on the normal backup cycle.

Network and platform hardening

The consoles apply a strict content security policy, frame protection, no sniff content type, referrer policy and a restrictive permissions policy. Administrative and provisioning endpoints are protected by shared secrets or signed tokens.

Operational security

We follow least privilege for administrative access, keep credentials out of source control, store live keys in an encrypted vault, and separate production from development. Automated monitoring watches the platform and its supporting automation, with alerting to the operations team.

Sub-processors

We use vetted providers that maintain recognised security programmes. See Annex III of the Data Processing Agreement for the list.

Incident response

If we become aware of a security incident affecting personal data, we investigate, contain and remediate, and notify affected Customers without undue delay with the information available, so they can meet their own obligations.

Responsible disclosure

If you believe you have found a security vulnerability, please contact ops@algozgroup.com with details so we can investigate. Please do not access or modify data that is not yours and do not run tests that could disrupt the service.