QuestWorks for Slack — Security & IT Summary

Slack app for 25-min team development sessions · v1.0 · 2026-05-06 · asa@questworks.io

What it is: QuestWorks is a Slack app that schedules and runs 25-minute browser-based group sessions, then provides managers with team dynamics insights from in-session behavior. Standard Slack OAuth install. No desktop client, no plugins, no extensions. Hosted on Render (Node.js bot), Netlify (dashboard + install pages), and Supabase (Postgres + auth + storage). All infrastructure in US regions.

SLACK OAUTH SCOPES (12 TOTAL, LEAST-PRIVILEGE)

`chat:write`	Post quest invites, session reminders, leaderboards into the dedicated #questworks channel and player DMs
`commands`	Register slash commands: `/onboard`, `/dashboard`, `/questnow`, `/admin`, `/summon`, `/reschedule`, `/world`, `/report`, `/settings`
`im:write / im:read`	DM invited players for magic-link onboarding and post-session reports; read DM channel metadata for 1:1 conversations
`channels:read / :join / :manage / :write.invites`	Find, join, recover (unarchive), and invite players into the dedicated #questworks announcement channel created at install
`users:read / users:read.email`	Resolve display names for leaderboard and `/summon`; read installer email at OAuth for setup-confirmation emails
`app_mentions:read`	Receive events when the bot is @-mentioned in a channel
`files:read`	Upload data-export and consent-history files into a player's DM (GDPR/CCPA "Download My Data")

QuestWorks does **not** request `chat:write.public`, `groups:write`, `files:write`, message-history scopes (`channels:history`, `im:history`, etc.), or any admin-tier scopes. The bot cannot read message content in any channel.

WHAT WE ACCESS

- **Slack:** profile (name, email, photo, timezone), channel list metadata, membership of the #questworks channel, DMs we open
- **Browser session (during 25-min quest):** mic audio (real-time only), webcam via LiveKit (relay only), gameplay inputs, dice rolls, response timing
- **Google Calendar (OAuth, optional):** free/busy windows during stated playing hours, read/write of QW-created events only (scoped via `calendar.events`)
- **Productivity tools (manager opt-in):** task metadata only from Linear, GitHub, Jira, Asana, Monday, ClickUp, Figma, Notion, HubSpot, CultureAmp, Lattice, 15Five — never source code or document contents

WHAT WE STORE

- **Supabase Postgres (US):** profile, session history, behavioral tags, gear/loot inventory, XP/level, certifications, full consent audit trail, single-use magic-link tokens
- **Redis (US, ephemeral):** live session state during the quest — wiped at session end
- **Supabase Storage:** generated character portraits, quest backdrops
- **Retention:** data kept for life of subscription; full deletion within 30 days of uninstall or cancellation (sooner on request); consent audit logs retained 7+ years per GDPR Article 7(1)

Voice & video: Player audio is streamed in real time to Deepgram for transcription. **Audio itself is never stored** — only the resulting text transcript. Webcam streams are relayed via LiveKit and **never recorded**. Players grant explicit Recording Consent at onboarding; one-click withdrawal in `/settings` immediately disables future session invites.

SECURITY POSTURE

- TLS 1.2+ on all endpoints; AES-256 at rest (Supabase default for Postgres, storage, and backups)
- Postgres Row-Level Security on all player-scoped tables; service-role key restricted to server-side environment, never exposed client-side
- Magic-link auth: single-use tokens, atomic redemption, 24h expiry; dashboard sessions via short-TTL JWT
- HMAC verification on all webhooks (Slack signing secret, Stripe-Signature, Resend via Svix); OAuth refresh tokens encrypted at rest
- Supabase Security Advisor sweep completed 2026-04: 108 of 110 findings remediated, remaining 2 documented as accepted-risk by design

COMPLIANCE & ADMIN CONTROLS

- **GDPR + CCPA** supported in-product via `/settings`: View My Data, Download My Data (full JSON export), Consent Settings (per-type grant/withdraw), Delete Profile, Export Consent History (JSON + human-readable)
- **Workspace admins** can uninstall via Slack admin panel — immediately revokes OAuth tokens; on uninstall, all data deleted within 30 days
- Per-player invite pause via `/settings` without affecting workspace install
- `/admin` panel with 22 sub-controls for player management, session settings, billing, data export
- DPA available on request · Privacy: questworks.io/privacy-policy · Terms: questworks.io/terms · Contact: privacy@questworks.io

SUBPROCESSORS (ALL US-REGION)

Supabase (DB/auth/storage) · Render (hosting) · Netlify (dashboard) · Stripe (billing, tokenized) · Resend (email) · Google Gemini (LLM, no training opt-in) · Google Imagen 4 (avatars, prompts only) · Hume (NPC TTS) · Deepgram (transcription) · LiveKit (A/V, no recording) · Google Calendar · Grafana Cloud (observability, PII redacted) · Linear (bug routing). Manager-opt-in only: GitHub, Jira, Asana, Monday, ClickUp, Figma, Notion, Google Workspace, HubSpot, CultureAmp, Lattice, 15Five, LinkedIn.

Pricing: $20/seat/month, billed monthly, no annual commitment. **10-day free trial, no credit card required** — full features, one quest per player, per-team isolation in multi-team workspaces. · **Founder:** Asa Goldstein, asa@questworks.io — happy to jump on a 15-min call for any IT/security question.