QuestWorks for Microsoft Teams — Security & IT Summary

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

What it is: QuestWorks is a Microsoft Teams app that schedules and runs 25-minute browser-based group sessions, then provides managers with team dynamics insights from in-session behavior. Installed via Bot Framework with tenant admin consent. 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.

MICROSOFT GRAPH PERMISSIONS (4 TOTAL, APPLICATION-LEVEL, ADMIN CONSENT)

`Calendars.ReadWrite`	Auto-schedule sessions, run `/questnow`, sync RSVPs, and check free/busy. QuestWorks only writes events with its own organizer ID and never modifies events it didn't create. (Scopable to a security group via Application Access Policy — see below.)
`Channel.Create`	Create the dedicated #QuestWorks channel in the host team at install time
`ChannelSettings.ReadWrite.All`	Set channel description and privacy settings on the QuestWorks channel only — never modifies other channels
`User.Read.All`	Resolve display names and emails for the `/summon` command and onboarding flow (read-only basic profile fields)

QuestWorks does **not** request `Mail.*`, `Files.*`, `Sites.*`, `ChatMessage.*`, `Chat.ReadWrite`, or `Directory.ReadWrite.All`. Cannot read mail, access SharePoint/OneDrive, read message content in any channel or chat, or modify the directory. Bot Framework manifest registers messaging, adaptive cards, task modules, and proactive notifications. Slash commands: `/onboard`, `/dashboard`, `/questnow`, `/admin`, `/summon`, `/reschedule`, `/world`, `/report`, `/settings`.

WHAT WE ACCESS

- **Microsoft Teams:** profile (AAD object ID, display name, email, photo), the host team's #QuestWorks channel created at install, 1:1 chats the bot opens with players
- **Browser session (during 25-min quest):** mic audio (real-time only), webcam via LiveKit (relay only), gameplay inputs, dice rolls, response timing
- **Microsoft Graph (admin-consented):** free/busy windows, QW-created calendar events only, basic user profile via `User.Read.All`
- **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 (Bot Framework signing, Stripe-Signature, Resend via Svix); Graph subscription dead-man's-switch monitoring; 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)
- **Tenant admins** can uninstall via the Teams admin center — immediately revokes admin consent and all tokens; on uninstall, all data deleted within 30 days
- **Application Access Policy:** scope `Calendars.ReadWrite` to a specific security group to restrict QuestWorks to a pilot cohort
- Per-player invite pause via `/settings` without affecting tenant 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) · Microsoft Graph (calendar + directory) · 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 tenants. · **Founder:** Asa Goldstein, asa@questworks.io — happy to jump on a 15-min call for any IT/security question.