Security Summary

TeamTalk is a UK-hosted service that delivers workplace notices to frontline workers in their own language and records confirmation of receipt. This summary is written for a customer's IT, information security or data protection reviewer. Values in [square brackets] are confirmed per deployment before issue.

Supplier	[TeamTalk Ltd], company number [number], registered at [registered office]. ICO registration [registration number].
Service	TeamTalk, a multi-tenant software as a service application at [customer].team-comms.com
Role under UK GDPR	Processor. The customer is the controller of worker personal data.
Security contact	[security@team-comms.com] · [mobile] · monitored [08:00 to 18:00 UK, Monday to Friday]
Certifications	Cyber Essentials, certificate [cert no.], issued [date], expires [date]. Cyber Essentials Plus [held / not held / planned]. Not certified to ISO/IEC 27001; a written information security management roadmap is available on request.

Architecture and hosting

- **Application:** Laravel 11 (PHP) with Livewire 3, HTTPS only, delivered to workers as an installable progressive web app with web push (VAPID). No native mobile app, no app store.
- **Data stores:** MySQL for application data; Redis for cache, sessions and queues; Amazon S3 for files, photographs and exports.
- **Real time:** WebSocket messaging via [self-hosted Laravel Reverb / Pusher Channels]. Self-hosted Reverb means no third party sees message content.
- **Hosting:** Amazon Web Services, **eu-west-2 (London)**. Servers provisioned through Laravel Forge, which holds deployment credentials but stores no customer data.
- **Network exposure:** only 443 (HTTPS) and [22] (SSH, key and source-address restricted) are internet-facing. Databases and Redis are not. AWS console access requires multi-factor authentication.
- **Environments:** separate production and [staging]. Production personal data is never copied into non-production environments.

Encryption

- **In transit:** TLS 1.2 or above on all connections, certificates issued and renewed automatically by Let's Encrypt, HTTP redirected to HTTPS, HTTP Strict Transport Security enabled.
- **At rest:** AES-256 on Amazon EBS volumes and S3 buckets using AWS-managed keys. Backups use the same mechanism.
- **Secrets:** application secrets and API keys are held in environment configuration on the server, never in source control. Administrator passwords are bcrypt hashes and are not recoverable.
- **Uploads:** photographs and files are stored in S3 with private access, served through short-lived signed URLs, and are not publicly listable.

Authentication and access control

CONTROL	HOW IT WORKS
Worker sign-in	Mobile number plus a single-use, time-limited code delivered by SMS through Twilio Verify. No worker password and no email address, which removes the two most common frontline credential risks: shared passwords and password reuse.
Session lifetime	Sessions persist for up to 30 days so a worker is not asked for a code at every shift. **Recommended hardening:** bind each session to the device that created it, so a stolen cookie cannot be replayed elsewhere, and invalidate all of a user's sessions when their phone number changes.
Administrator roles	Administrator, moderator and worker roles within each tenant, assigned by a tenant administrator.
Support access and impersonation	A landlord administration function creates tenants and, where necessary for support, impersonates a user. **Every impersonation is logged with the operator, the impersonated user, the tenant and the timestamp**, and the log is available to the customer on request.
Leaver control	Each worker record carries a leaving date. Access is revoked on that date, including mid-session. This closes the most common gap in WhatsApp-based site communication.
TeamTalk staff access	Production access is limited to named personnel on least privilege, uses individual rather than shared accounts, and is protected by multi-factor authentication and SSH keys. Administrative accounts are kept separate from day-to-day accounts. Access is reviewed [quarterly] and removed on the day a person leaves. All personnel are bound by written confidentiality obligations surviving their engagement, are briefed on security at least annually, and are subject to right to work checks.

Tenant isolation

Each customer is a separate tenant with its own subdomain or custom domain, branding and users. Every record carries a tenant identifier and every query is scoped to the tenant resolved from the request domain, enforced globally in the application layer rather than left to individual queries. File storage is partitioned by tenant, so a user in one tenant cannot enumerate, read or address users, posts or files in another. Dedicated-database deployment is available to enterprise customers on request.

Backups, restore and continuity

- **Backup frequency:** database backed up [daily], encrypted, stored in Amazon S3 in the same UK region with versioning enabled.
- **Retention:** [30] days, then deleted automatically.

- **Restore testing:** full restore to a scratch environment [quarterly], with date, duration and outcome recorded.
- **Recovery time objective:** [4] hours for the application from a confirmed loss of the production server.
- **Recovery point objective:** [24] hours, or [5 minutes] where point-in-time recovery is enabled on the managed database.
- **Continuity:** infrastructure is reproducible through Laravel Forge, so a replacement server can be provisioned and the most recent backup restored without manual rebuilding.
- **Key person risk:** credentials for all critical systems are held in [a password manager] with a documented emergency access arrangement held by [named person or solicitor].

Monitoring, logging and vulnerability management

- **Uptime monitoring** from outside the network at [1 minute] intervals, alerting the on-call engineer by [email and SMS].
- **Error and exception monitoring** in the application, with alerting on new and repeated errors.
- **Audit logging** of administrator actions, impersonation, account creation and deletion, leaving-date changes, and publication and deletion of posts.
- **Operating system updates** are applied through the hosting platform with unattended security updates enabled. Critical and high severity updates are applied **within 14 days of release**, the Cyber Essentials requirement, and within [72 hours] where a vulnerability is actively exploited.
- **Dependency management:** PHP and JavaScript dependencies are reviewed and updated [monthly], with automated vulnerability alerts. Unsupported software is removed or upgraded before end of support.
- **Secure development:** changes go through source control and deploy from a protected branch. Framework protection against SQL injection, cross-site scripting and cross-site request forgery is on by default and is not disabled.
- **Penetration testing:** [an independent external test was carried out by [supplier] on [date]; the summary report and remediation status are available under a mutual non-disclosure agreement].

Incident response and breach notification

TeamTalk maintains a written incident response procedure with a single named owner. On becoming aware of an incident affecting a customer's data it will contain and assess it; **notify the affected customer without undue delay and in any event within 24 hours** where personal data is involved, so the customer as controller can meet its own 72-hour duty under Article 33(1) of the UK GDPR; supply what that notification needs, being the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences and the measures taken; assist with any notification to individuals; and issue a written post-incident report within [10] working days. It does not notify the Commissioner on the customer's behalf unless instructed in writing.

Sub-processors and international transfers

SUB-PROCESSOR AND LOCATION	WHAT IT DOES, WHAT IT RECEIVES, AND THE ROUTE FOR ANY TRANSFER OUTSIDE THE UK
Amazon Web Services United Kingdom, eu-west-2	Hosting, database, object storage and backups. Receives all customer data. No transfer outside the UK for hosted data; the region is contractually controlled. Support access from outside the UK runs on the AWS UK GDPR Addendum.
Twilio Inc. United States	SMS delivery of one-time sign-in codes, and of posts where enabled. Receives the mobile number, and the message text where SMS delivery of posts is used. Transfer runs on the **UK Extension to the EU–US Data Privacy Framework**, under which Twilio Inc. is actively certified, so no separate transfer agreement or risk assessment is needed.
OpenAI OpCo, LLC United States	Machine translation of post text, captions and comments. Receives **post content only**: no name, phone number, email address or user identifier. OpenAI is not certified under the Data Privacy Framework, so the transfer runs on the **ICO's International Data Transfer Addendum (B1.0) to the EU Standard Contractual Clauses**, with a documented transfer risk assessment. API data is retained for up to 30 days for abuse monitoring and is not used to train models.
Mux, Inc. United States	Video ingest, encoding, storage, delivery and automatic captions. Receives video and audio published by the customer. Transfer runs on the **UK Extension to the EU–US Data Privacy Framework**, with the ICO Addendum as Mux's contractual fallback.
Pusher (optional) [EU cluster]	Real-time delivery of updates in the browser, used only where self-hosted Laravel Reverb is not deployed. Receives message payloads and channel identifiers. Pusher is not on the Data Privacy Framework list. [State the mechanism once the cluster and entity are fixed.]
[Mailgun Technologies, Inc. / Amazon SES] [US / EU / UK]	Transactional email to administrators. Receives email address, name and message content. [Mailgun Technologies, Inc. is actively certified under the UK Extension to the DPF; Amazon SES is covered by the AWS UK GDPR Addendum. State which is in use.]

The current list is at [https://team-comms.com/sub-processors]. Customers get at least 30 days' notice of any new or replacement sub-processor and may object on reasonable data protection grounds, as the data processing agreement sets out. The list is deliberately short: minimising the number of parties that touch worker data is a design decision.

Data retention and deletion

Posts, confirmations of receipt, compliance exports, hazard reports and photographs: [24] months, configurable per tenant, then deleted automatically. **Worker records:** until the leaving date, on which access is revoked, then [12] months for evidential purposes. **Backups:** [30] days; data deleted from the live system persists in backups only until the backup expires and is never restored into it. **Logs:** [90] days. **Whole tenant on termination:** 30 days for export, then deleted within a further 30 days, with written confirmation. **Individual rights requests** are handled by the customer as controller, using tools TeamTalk provides to locate, export and delete a record, with TeamTalk assisting within [5] working days.

Accuracy. Confirm every bracketed value against the live deployment before sending this to a customer. **Sources, verified 28 August 2026:** UK GDPR Arts 28, 32, 33 and Chapter V as amended, legislation.gov.uk/eur/2016/679; ICO international transfer tools, IDTA A1.0 and Addendum B1.0, in force 21 March 2022, ico.org.uk; UK Extension to the EU–US Data Privacy Framework, SI 2023/1028, in force 12 October 2023, participant statuses from dataprivacyframework.gov/list; Cyber Essentials Requirements for IT Infrastructure v3.3, ncsc.gov.uk.