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.

HOW TO COMPLETE THIS DOCUMENT, AND THE ONLY RULE THAT MATTERS

Tick only what is true today; write "not yet" for the rest. A box left unticked or marked NOT YET costs nothing: reviewers expect a young supplier to have gaps and they respect a supplier who names them. A tick that turns out to be false costs the account and the relationship, and every answer here becomes a contractual representation the moment it is sent. Where the answer is "not yet", give the date by which it will be true. Do not send this document with an unresolved [bracket] in it.

WHAT A CONFIRMATION RECORD IS, AND WHAT IT IS NOT

The Service records that a person confirmed a notice. That is evidence of an act, not of comprehension, and it does not by itself discharge any duty under health and safety, food safety or other law. TeamTalk does not provide legal advice.

The supplier

Supplier	[TeamTalk Ltd], company number [number], registered at [registered office]. ICO registration [registration number].
Scale, stated plainly	**One director, no employees, pre-revenue.** Where this document names a role or a review cycle that a second person would carry out, it takes effect when that person is engaged. External escalation route: [accountant / solicitor, name and telephone].
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.
Hosting	**United Kingdom (AWS London, eu-west-2).** This is a commitment in the data processing agreement, not a configuration preference.
Security contact	[security@team-comms.com] · [mobile] · monitored [08:00 to 18:00 UK, Monday to Friday]. **There is no 24/7 on-call rota and none is claimed.**
Certifications	**Cyber Essentials: not currently held. Assessment booked with [body], target [date].** Cyber Essentials Plus: not held. Not certified to ISO/IEC 27001 and does not claim to be; a written information security management roadmap is available on request.
Site visits	TeamTalk staff visit customer premises for onboarding and training only, under the customer's site rules and induction; no construction or operational work is carried out.

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. All in the United Kingdom (AWS London, eu-west-2).
☐ **Real time**	**Self-hosted Laravel Reverb**, so no third party sees message content. [Pusher only if enabled; if it is, say so and state the cluster.]
☐ **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.
☐ **Provisioning**	Servers provisioned through Laravel Forge, which holds deployment credentials but stores no customer data and is not a sub-processor.

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. [Confirm the HSTS header and its max-age.]
☐ **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 held in environment configuration on the server, never in source control. Administrator passwords are bcrypt hashes and are not recoverable.
☐ **Uploads**	Photographs and files stored in S3 with private access, served through short-lived signed URLs, not publicly listable.

Authentication and access control

Two different things are described here and they are deliberately kept apart, because a reviewer who finds them conflated will discount the whole document.

☐ **Administrator and staff sign-in: multi-factor, true today**	**Multi-factor authentication is enforced on every cloud service account TeamTalk holds**, including AWS, the deployment platform, the source code repository and every third-party service, and on TeamTalk staff access to production, which also uses individual named accounts and SSH keys on least privilege. This is genuine MFA: something known plus something held.
☐ **Worker sign-in: single-factor possession, and said so**	A worker signs in with a mobile number and a single-use, time-limited code delivered by SMS through Twilio Verify. There is no worker password. **That is single-factor possession, not multi-factor authentication, and TeamTalk does not call it MFA.** It is defensible on its merits for a frontline workforce: **there is no password to phish, share or reuse**, which removes the two commonest frontline credential risks; the factor is **per-device and per-number**, so it cannot be passed round a site the way a shared password is; and the code is **short-lived and single-use**. The residual risk is loss of the handset, which is mitigated by the leaver control below and by invalidating sessions on a change of number.
☐ **Session handling**	PLANNED BEFORE FIRST CUSTOMER Binding each session to the device that created it, invalidating all of a user's sessions when their mobile number changes, and setting the session lifetime deliberately rather than by framework default. **Do not tick this until it ships.**
☐ **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.
☐ **Personnel measures**	As at [date] there are no employees, so these apply to the director today and to each person engaged from the day they are engaged: written confidentiality obligations surviving engagement, right to work check before starting, security briefing on joining and at least annually, access removed on the last working day, access reviewed [quarterly].

Tenant isolation

☐ **Isolation model**	**Logical tenant isolation enforced at the data layer, with automated cross-tenant tests** NOT YET **.** 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. A user in one tenant cannot enumerate, read or address users, posts or files in another. **The Service is multi-tenant; it is not single-tenant and is not described as such.** Dedicated-database deployment is available to enterprise customers on request.
☐ **Automated cross-tenant tests**	NOT YET A test suite that asserts a user in tenant A cannot read, list or address anything in tenant B, run on every deploy. Target [date]. Tick this row and cite the tests by name once they exist; this is the question a security reviewer asks twice.

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. Last successful restore test: [date, or "not yet: first drill booked for [date]"].
☐ **RTO and RPO**	Recovery time objective [4] hours from a confirmed loss of the production server; recovery point objective [24] hours, or [5 minutes] where point-in-time recovery is enabled. **Give figures from a timed drill, not an estimate.**
☐ **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**	With one director this is the real risk and it is not hidden. Credentials for all critical systems are held in [a password manager] with a documented emergency access arrangement held by [named person or the company's solicitor]. On termination for any reason, including insolvency, customer data is available for export for 30 days.

Monitoring, logging and vulnerability management

☐ **Uptime monitoring**	From outside the network at [1 minute] intervals, alerting **the named director** by [email and SMS]. **There is no on-call engineer.**
☐ **Error monitoring**	In-application error and exception monitoring with alerting on new and repeated errors. [Name the tool. If it stores request payloads it is a sub-processor and must be listed below.]
☐ **Audit logging**	Administrator actions, impersonation, account creation and deletion, leaving-date changes, and publication and deletion of posts. Retained [90] days.
☐ **Patching**	Unattended security updates enabled. Critical and high severity updates, or CVSS v3 base score 7 or above, applied **within 14 days of release**, which is the Cyber Essentials requirement, and within [72 hours] where a vulnerability is actively exploited.
☐ **Dependencies**	PHP and JavaScript dependencies reviewed and updated [monthly], with automated vulnerability alerts. Unsupported software 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**	[Not yet carried out. Booked with [supplier] for [date].] If a test has been done, name the supplier, the date and the remediation status, and offer the summary report under a mutual non-disclosure agreement. A scheduled date is a credible answer; a blank is not.

Incident response and breach notification

TeamTalk maintains a written incident response procedure with a single named owner, who is the director. 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. Notification runs to the named contact by telephone and email, not through a portal.

Sub-processors and international transfers

Every Data Privacy Framework status below was checked against the official participant list at dataprivacyframework.gov/list on **28 August 2026**. Certifications lapse, so these are **re-checked every six months** and before answering any questionnaire.

SUB-PROCESSOR AND CONTRACTING ENTITY	WHAT IT DOES AND WHAT IT RECEIVES	COUNTRY	TRANSFER BASIS, CHECKED 28 AUG 2026
Amazon Web Services [AWS EMEA SARL]	Hosting, database, object storage and backups. Receives all customer data.	**United Kingdom** AWS London, eu-west-2	**No transfer for hosting.** Data at rest stays in the UK; the region is contractually controlled. Support access from outside the UK runs under Article 46 on the **AWS UK GDPR addendum**. AWS makes no Data Privacy Framework claim in its contract documents, so the addendum is the operative route.
Twilio Inc.	SMS delivery of one-time sign-in codes, and of posts where enabled. Receives the mobile number, and message text where SMS delivery is used.	United States	**Article 45A, UK Extension to the EU–US Data Privacy Framework.** Listed **Active**. No separate transfer agreement or risk assessment needed.
Mux, Inc.	Video ingest, encoding, storage, delivery and automatic captions. Receives video and audio published by the customer.	United States	**Article 45A, UK Extension**, but listed **Active, re-certification under review**. Said here rather than left for a reviewer to find: this is the one status in the list that can lapse. The ICO Addendum is Mux's contractual fallback and TeamTalk will move to it if the status changes.
OpenAI OpCo, LLC	Machine translation. **Post text, comment text, direct message text and hazard report text are sent for translation. No names, phone numbers or identifiers accompany the text.**	United States	**No Data Privacy Framework certification** (0 of 7,567 records). Transfer runs on **Article 46** via the ICO's **International Data Transfer Addendum (B1.0)** or the IDTA (A1.0), with a documented **transfer risk assessment**. API data retained up to 30 days for abuse monitoring and not used to train models.
Transactional email [Amazon SES / Mailgun, confirm which]	Transactional email to administrators. Receives email address, name and message content.	[UK if SES / US if Mailgun]	[Confirm which is configured.] Amazon SES in eu-west-2 is covered by the AWS UK GDPR addendum under Article 46. Mailgun Technologies, Inc. is listed **Active** for the UK Extension, so Article 45A applies to that entity only.

SUB-PROCESSOR AND CONTRACTING ENTITY	WHAT IT DOES AND WHAT IT RECEIVES	COUNTRY	TRANSFER BASIS, CHECKED 28 AUG 2026
Real-time delivery [self-hosted Reverb; Pusher only if enabled]	Real-time delivery of updates in the browser.	[UK, TeamTalk's own servers]	Where **Laravel Reverb is self-hosted there is no sub-processor and no transfer**. Pusher is engaged only if enabled; it does not appear on the Data Privacy Framework list, so a basis must be stated before it processes anything. [Delete this row if Reverb is self-hosted.]

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, not an accident of scale.

Data retention and deletion

These are the defaults in clause 4.7.5 of the data processing agreement, where they are contractual rather than descriptive. **The controller may instruct otherwise. Posts, comments, translations and confirmation records, including briefing record exports:** 24 months after the end of the relationship, then deleted automatically. **Worker accounts:** deactivated on the recorded leaving date; identifiers minimised 12 months after that date. **Hazard reports and photographs:** 24 months. **Logs, including the impersonation log:** 90 days. **Backups:** [30] days; data deleted from the live system persists in backups only until the backup expires and is never restored into it. **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.

Worker monitoring, named rather than buried

Per-worker sign-in timestamps, confirmation records and chase lists are **monitoring of workers** within the meaning of the Information Commissioner's employment practices guidance. TeamTalk names it rather than waiting to be asked. The customer is the controller and is responsible for the lawful basis, the transparency information and the proportionality assessment; TeamTalk supplies a **pre-completed DPIA and monitoring pack** and a **worker privacy notice template** to make that straightforward. **What the Service does not do, and has no feature for: no location tracking, no message-content analysis, no productivity scoring.**

Accuracy. Tick only what is true today and write "not yet" for the rest. Confirm every bracketed value against the live deployment before sending this to a customer. Every answer here becomes a contractual representation once sent. **Sources, verified 28 August 2026:** UK GDPR Arts 28, 32, 33 and Chapter V as substituted with effect from 5 February 2026, legislation.gov.uk/eur/2016/679; Data (Use and Access) Act 2025 s.85 and Sch. 7, commenced by SI 2026/82; 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 read from dataprivacyframework.gov/list on 28 August 2026; ICO, *Employment practices and data protection: monitoring workers*, ico.org.uk; NCSC, *Cyber Essentials: Requirements for IT Infrastructure v3.3*, ncsc.gov.uk.