Business Continuity Summary

How [TeamTalk Ltd] keeps the TeamTalk service running, and what happens if it cannot. Written for a customer's continuity or procurement reviewer.

SCALE NOTE
As at [date] TeamTalk has **one director and no employees**. Where this policy names a second role or a review cycle, it takes effect when that person is engaged. External escalation: [accountant / solicitor, name and telephone].

1. Purpose and scope

This summary describes how [TeamTalk Ltd] maintains the TeamTalk service through disruption, and how it recovers if the service is lost. It covers the production environment, the company's people and its critical suppliers. The full plan is held at [location] and is available to a customer under a confidentiality undertaking.

The company is small and says so. This plan is written for a business of that size: it depends on reproducible infrastructure and tested backups rather than on standby sites and duty rotas that a company of this size cannot staff.

2. Recovery objectives

OBJECTIVE	TARGET
Recovery time objective (application)	[4] hours from a confirmed loss of the production server
Recovery point objective (data)	[24] hours, or [5 minutes] where point-in-time recovery is enabled
Maximum tolerable period of disruption	[24] hours
Backup frequency and retention	[Daily], encrypted, retained [30] days in the same UK region
Restore testing	[Quarterly] full restore to a scratch environment, with date, duration and outcome recorded

3. Scenarios and response

1. **Loss of the production server or environment.** Infrastructure is defined and reproducible through the deployment platform, so a replacement server can be provisioned into the same UK region and the most recent encrypted backup restored, without manual rebuilding. Customers are told the position and given an estimated restoration time as soon as the assessment is complete, and are updated at agreed intervals until service is restored.
2. **Data loss or corruption.** Restore from the most recent good backup, to the recovery point objective above. Object storage is versioned so that an accidental deletion or overwrite can be reversed without a full restore.
3. **Loss of a critical third-party service.** Loss of SMS delivery removes new sign-ins but not access for workers who already have a live session. Loss of translation degrades gracefully: posts publish in the language they were written in rather than failing. Loss of video affects video posts only. Loss of push notification delivery leaves posts readable in the application. **The service is designed so that a third-party failure degrades a feature rather than stopping the platform.**
4. **Loss of premises.** The company is remote-first and has no operational dependency on a building. Work continues from any location with an internet connection.
5. **Loss of key personnel.** This is the company's most significant continuity risk and is not disguised. Credentials for every critical system are held in [a password manager], with a documented emergency access arrangement held by [named person or the company's solicitor]. Infrastructure, deployment and recovery procedures are documented so that a competent engineer can operate the service without the original author. [A named external engineer, [name], is retained and briefed as a contingency.]
6. **Cyber incident.** Handled under the incident response procedure: contain, assess, notify the affected customer without undue delay and within 24 hours where personal data is involved, restore from a known-good backup, and issue a written post-incident report within [10] working days.
7. **Insolvency or cessation of trading.** Customer data remains available for export in a machine-readable format for 30 days from termination for any reason. The obligation is written into the customer agreement so that it survives the commercial relationship.

4. Communication during an incident

Each customer has a named contact and each has named a contact within its own organisation. During a disruption the company communicates by telephone and email to that person, gives the facts it has confirmed rather than waiting for a complete picture, and states when the next update will come. Status is also published at [status page URL]. The company does not use the affected platform as its only channel for telling customers that the platform is affected.

5. Testing, review and honest limitations

The restore procedure is tested [quarterly] and the incident response procedure is walked through [annually], with findings recorded and acted on. This summary is reviewed at least annually and after any incident or material change to the architecture.

What this plan does not claim. There is no hot standby environment and no automatic failover to a second region. There is no 24-hour staffed operations centre. The company is not certified to ISO 22301. These are the honest limits of a business of this size, and a customer requiring more should say so during evaluation, when the cost of providing it can be discussed, rather than discovering it during an incident.

Approved on behalf of [TeamTalk Ltd], company number [number], registered office [address].

SIGNATURE	NAME AND POSITION	DATE OF ISSUE	DATE OF NEXT REVIEW

Not legal advice. The recovery objectives below are targets. Do not send this to a customer until each has been evidenced by a timed drill, because the recovery time objective is the single answer procurement most often follows up on. **Sources, verified 28 August 2026:** UK GDPR Article 32(1)(b) and (c), which require the ability to ensure ongoing availability and resilience and to restore availability and access to personal data in a timely manner after an incident legislation.gov.uk/eur/2016/679/article/32; NCSC, Cyber Essentials, which recommends but does not require backup ncsc.gov.uk/cyberessentials/overview; ISO 22301 referenced as a framework only, and not held.