Information Security Policy

The information security commitments of [TeamTalk Ltd], aligned to the five Cyber Essentials technical control areas and to Article 32 of the UK GDPR.

1. Policy statement

[TeamTalk Ltd] holds personal data belonging to other organisations' workforces, including names, mobile numbers and records of what each person was told and when. Those records are relied on as evidence. The company protects the confidentiality, integrity and availability of that information, and holds itself to the technical standard set by **Cyber Essentials** and to the requirement in Article 32 of the UK GDPR to implement measures appropriate to the risk.

The company is certified to Cyber Essentials, certificate [number], expiring [date]. It is **not certified to ISO/IEC 27001 and does not claim to be**; a written roadmap is available on request.

2. Scope

This policy applies to all information the company holds, in any form, and to every employee, director and contractor, and to every device and cloud service used for company work, wherever located. Compliance with it is a condition of engagement.

3. The five controls

1. **Firewalls.** Every internet-facing system is behind a correctly configured firewall that blocks unauthenticated inbound connections by default. Inbound rules are documented with a business need, approved by a named person, and removed when no longer needed. Devices used outside the office rely on a software firewall on the device, because home routers are outside the company's control.
2. **Secure configuration.** Default and guessable passwords are changed. Unnecessary accounts, software and services are removed or disabled. Devices lock automatically. Users are authenticated before reaching any company data.
3. **Security update management.** All software is licensed and supported; unsupported software is removed or upgraded before end of support. Automatic updates are enabled. Updates for vulnerabilities rated critical or high, or scoring 7 or above on CVSS v3, are applied **within 14 days of release**.
4. **User access control.** Access is granted on least privilege, through individual named accounts, on a documented approval, and is reviewed [quarterly] and removed on a person's last working day. **Multi-factor authentication is enabled on every cloud service account.** Administration is done from accounts used only for administration, never for email or browsing.
5. **Malware protection.** Every device runs malware protection that is kept updated, or is restricted to signed, allow-listed applications.

4. Protecting customer data specifically

- **Encryption.** TLS 1.2 or above in transit; AES-256 at rest, including backups.
- **Tenant isolation.** Every record carries a tenant identifier and every query is scoped to the tenant resolved from the request domain, enforced globally rather than left to individual queries.
- **Support access.** Impersonation of a user for support is restricted to named personnel and is logged in full, with the log available to the customer.
- **Data minimisation.** Only the text of a post is sent for translation; no names, numbers or identifiers leave the platform for that purpose. All data at rest stays in the United Kingdom.
- **Backups.** Encrypted, held in the same UK region, retained [30] days, and restore-tested [quarterly] with the result recorded.
- **Secure development.** Changes go through source control and deploy from a protected branch. Framework protections against injection and cross-site attacks are not disabled. Production personal data is not copied into development or staging environments.

5. People

Right to work checks are carried out on all staff. Everyone is bound by written confidentiality obligations that survive the end of their engagement, is briefed on security and data protection on joining and at least annually, and has all access removed on their last working day. Deliberate misuse of company or customer information is gross misconduct, and unauthorised access to a computer system is a criminal offence under the Computer Misuse Act 1990.

6. Incidents

Everyone must report a suspected security incident or data breach immediately to [name, email, mobile], however minor it appears and however it arose. **Nobody will be criticised for reporting an incident, including one they caused.** The company follows a written incident response procedure and notifies an affected customer without undue delay and in any event within 24 hours where personal data is involved, so the customer can meet its own duty to the Information Commissioner under Article 33.

7. Responsibility and review

[Name, Director] owns this policy and information security generally. It is reviewed at least annually, on any material change to the service or the estate, before each Cyber Essentials renewal, and after any 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. This is the short, issuable version. The detailed technical measures are in the security summary and in Annex 2 of the data processing agreement, and the two must not contradict each other: update them together. **Sources, verified 28 August 2026:** NCSC, Cyber Essentials, and *Cyber Essentials: Requirements for IT Infrastructure v3.3*, April 2026 ncsc.gov.uk/cyberessentials/overview; IASME Cyber Essentials scheme and the Danzell question set iasme.co.uk/cyber-essentials; UK GDPR Articles 5(1)(f) and 32 (security of processing), and Article 33 (breach notification) legislation.gov.uk/eur/2016/679/article/32; Data Protection Act 2018 legislation.gov.uk/ukpga/2018/12; Computer Misuse Act 1990 legislation.gov.uk/ukpga/1990/18.