

## Supplier questionnaire: answer bank

The sixty questions UK housebuilders, contract caterers and facilities management companies ask most often, with an answer written from TeamTalk's actual stack. Copy the answer, replace the [placeholders], and keep the filled-in version: the second questionnaire always takes a quarter of the time the first one did.

### HOW TO USE THIS, AND THE ONE RULE

Answers marked **VERIFY** contain a value that has never been measured or that changes over time. **Do not send a questionnaire with one of those still in it.** Confirm the number against the live deployment first. A wrong answer that a customer's IT team later discovers costs the deal and the relationship; a slow answer costs a day. Where the honest answer is "we do not do that", say so and give the date by which you will, which reads far better than a vague claim that unravels under a follow-up question.

### A · Company and commercial (1 to 8)

| QUESTION                                                     | ANSWER                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 Full registered name, company number and registered office | [TeamTalk Ltd], a private company limited by shares registered in England and Wales under company number [number], registered office [address]. Records are public at find-and-update.company-information.service.gov.uk.                                                |
| 2 Trading address and places of business                     | [address]. TeamTalk is a software supplier and does not carry out work on customer sites. No operatives, plant or vehicles attend site.                                                                                                                                  |
| 3 VAT registration number                                    | [GB number]. <b>OR STATE "NOT VAT REGISTERED" IF BELOW THE THRESHOLD; DO NOT LEAVE BLANK</b>                                                                                                                                                                             |
| 4 Date of incorporation and years trading                    | Incorporated [date]; trading since [date]. TeamTalk is an early-stage company, and says so rather than implying otherwise. References from current customers are available on request.                                                                                   |
| 5 Number of employees                                        | [N] employees and [N] contractors. <b>HEADCOUNT</b>                                                                                                                                                                                                                      |
| 6 Annual turnover and financial standing                     | Turnover for the year ended [date] was £[amount]. Accounts are filed at Companies House. TeamTalk has no county court judgments, is not in any insolvency procedure, and has no overdue statutory filings. <b>TURNOVER; CONFIRM THE FILING POSITION BEFORE ANSWERING</b> |
| 7 Bank details and payment terms                             | Bank details are supplied only through a verified channel, on request, and never by email alone. Standard terms are 30 days from invoice, by Bacs. TeamTalk does not accept payment by card as standard.                                                                 |
| 8 Named contacts                                             | Commercial and contract: [name, email, mobile]. Technical and security: [name, email, mobile]. Data protection: [name, email]. Escalation and incidents: [name, mobile], monitored [08:00 to 18:00 UK, Monday to Friday].                                                |

### B · Data protection and UK GDPR (9 to 22)

| QUESTION                                                | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9 Are you registered with the Information Commissioner? | Yes. Registration number [number], tier 1 (micro organisations), fee £52 a year, or £47 by direct debit. The entry is public on the ICO register. <b>REGISTRATION NUMBER AND RENEWAL DATE</b>                                                                                                                                                                                                                                                                                                          |
| 10 Are you a controller or a processor?                 | For the worker personal data in your tenant, <b>you are the controller and TeamTalk is the processor.</b> TeamTalk is a controller only for its own business contact data, billing records and service telemetry that does not identify your workers.                                                                                                                                                                                                                                                  |
| 11 What personal data will you process?                 | Name; mobile telephone number; optional email address; preferred language; employer or subcontractor; site, depot or team; group membership; role; start and leaving dates; the content of posts, comments and messages and their machine translations; video and captions; hazard reports including free text, location and photographs, which may show identifiable people; sign-in events; confirmations of receipt with timestamps; device and browser type; IP address; push notification tokens. |
| 12 Whose personal data?                                 | Your employees; your workers and agency staff; employees and operatives of your subcontractors working on your sites or contracts; your managers and administrators; and, incidentally, anyone appearing in a photograph or video published on the tenant.                                                                                                                                                                                                                                             |

| QUESTION                                                               | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 Do you process special category or criminal offence data?           | No. TeamTalk neither requires nor requests data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation, or criminal convictions. Preferred language is collected to deliver translation and is not used or inferred as a proxy for nationality or ethnicity. The data processing agreement prohibits the customer from using the service for such data.                                                                                                                                                                                                                                                                     |
| 14 What is the lawful basis?                                           | You determine it as controller. In practice it is normally legitimate interests, or compliance with a legal obligation where the communication discharges a statutory duty to inform or instruct. TeamTalk does not rely on consent for the operation of the service and does not use worker data for marketing.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 15 Will you sign a data processing agreement?                          | Yes. TeamTalk offers its own Article 28 compliant agreement, which can be signed the same day, and will review yours instead if you prefer. TeamTalk's version is available before contract so your data protection officer can read it during evaluation rather than at signature.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 16 Where is personal data stored and processed?                        | Amazon Web Services, region <b>eu-west-2 (London)</b> , in the United Kingdom. AWS will not move or replicate content outside the chosen region without agreement. <b>CONFIRM THE REGION FOR THIS DEPLOYMENT</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 17 Is any personal data transferred outside the UK, and on what basis? | All data at rest stays in the UK. Three sub-processors are in the United States. <b>Twilio</b> (SMS sign-in codes) and <b>Mux</b> (video) are certified under the <b>UK Extension to the EU-US Data Privacy Framework</b> , given effect by SI 2023/1028, so those transfers run on an adequacy route and need no transfer agreement or risk assessment. <b>OpenAI</b> (translation) is not certified, so that transfer runs on the ICO's <b>International Data Transfer Addendum, version B1.0</b> , supported by a documented transfer risk assessment carried out against the Article 46(6) test as amended by the Data (Use and Access) Act 2025. Only the text of a post is sent for translation: no names, numbers or identifiers. |
| 18 Do you have a data protection officer?                              | TeamTalk is not required to appoint one under Article 37 of the UK GDPR: it is not a public authority, its core activities do not consist of large-scale regular and systematic monitoring, and it does not process special category data at scale. A named individual is accountable for data protection: <a href="#">[name, email]</a> . This position is reviewed as the business grows.                                                                                                                                                                                                                                                                                                                                              |
| 19 How long is data retained, and how is it deleted?                   | Posts, confirmations and exports <a href="#">[24]</a> months, configurable per tenant. Worker records until the leaving date, then <a href="#">[12]</a> months. Hazard reports <a href="#">[24]</a> months. Backups <a href="#">[30]</a> days. Logs <a href="#">[90]</a> days. On termination, 30 days to export, then deletion within a further 30 days with written confirmation. <b>RETENTION PERIODS AND BACKUP RETENTION</b>                                                                                                                                                                                                                                                                                                        |
| 20 How do you support data subject rights requests?                    | Your administrators can locate, view, correct, export and delete an individual worker's record without contacting TeamTalk. Where more is needed, TeamTalk assists within <a href="#">[5]</a> working days of a written request, at no charge for ordinary volumes. If a data subject approaches TeamTalk directly it will not respond substantively but will forward the request to you without undue delay.                                                                                                                                                                                                                                                                                                                            |
| 21 What are your personal data breach notification timescales?         | TeamTalk notifies the affected customer <b>without undue delay and in any event within 24 hours</b> of becoming aware of a breach involving personal data, which is tighter than the Article 33(2) standard, so that you as controller have time to meet your own duty under Article 33(1) to notify the Commissioner without undue delay and where feasible within 72 hours. The notification carries the information Article 33(3) requires. A written post-incident report follows within <a href="#">[10]</a> working days. TeamTalk does not notify the Commissioner on your behalf unless instructed in writing.                                                                                                                   |
| 22 Will you assist with a data protection impact assessment?           | Yes. TeamTalk maintains a pre-completed assessment pack describing the processing, the data flows, the sub-processors and the risk mitigations, which your data protection officer can adapt. Supplying it up front routinely removes two to four weeks from procurement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## C · Information security (23 to 38)

| QUESTION                                       | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23 What security certifications do you hold?   | <b>Cyber Essentials</b> , certificate number <a href="#">[number]</a> , issued <a href="#">[date]</a> , expiring <a href="#">[date]</a> , assessed against the current IASME question set. Cyber Essentials Plus: <a href="#">[held / not held / planned for date]</a> . TeamTalk is <b>not</b> certified to ISO/IEC 27001 and does not claim to be; a written information security management roadmap is available, and divisions accept that alongside Cyber Essentials more often than suppliers expect. <b>CERTIFICATE NUMBER AND DATES</b> |
| 24 Do you have an information security policy? | Yes, a written policy owned by <a href="#">[name]</a> , reviewed annually and on material change, aligned to the five Cyber Essentials control areas. A copy is supplied on request. Every person with access to customer data is briefed on it on joining and at least annually.                                                                                                                                                                                                                                                               |

| QUESTION                                             | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25 Is data encrypted in transit and at rest?         | In transit: TLS 1.2 or above on all connections, certificates issued and renewed automatically, HTTP redirected to HTTPS, HTTP Strict Transport Security enabled. At rest: AES-256 on Amazon EBS volumes and S3 objects, including backups. <b>CONFIRM THE HSTS HEADER AND ITS MAX-AGE</b>                                                                                                                                                                                                                                                                                                                                                      |
| 26 How are encryption keys and secrets managed?      | Volume and object encryption uses AWS-managed keys. Application secrets and third-party API keys are held in server environment configuration, never in source control, and are rotated on personnel change and on suspicion of compromise. Administrator passwords are stored only as bcrypt hashes and are not recoverable.                                                                                                                                                                                                                                                                                                                   |
| 27 How is access to customer data controlled?        | Least privilege, individual named accounts rather than shared ones, and separate administrative accounts kept apart from day-to-day accounts. Production access is limited to <u>[N]</u> named people, protected by multi-factor authentication and SSH keys, reviewed <u>[quarterly]</u> and removed on a person's last working day. <b>NUMBER OF PEOPLE WITH PRODUCTION ACCESS, AND THE DATE OF THE LAST REVIEW</b>                                                                                                                                                                                                                           |
| 28 Is multi-factor authentication enforced?          | Yes, on every cloud service account TeamTalk holds, for administrators and ordinary users alike, including AWS, the deployment platform, the source code repository and every third-party service. This is now a mandatory Cyber Essentials requirement and is assessed as an automatic fail if it is not in place.                                                                                                                                                                                                                                                                                                                             |
| 29 What is your password policy?                     | Multi-factor authentication with a password of at least 8 characters and no maximum length, which is one of the three permitted Cyber Essentials options. Brute-force protection is in place. Password expiry is <b>not</b> enforced and complexity rules are <b>not</b> enforced, in line with NCSC guidance and the current scheme requirements.                                                                                                                                                                                                                                                                                              |
| 30 How do end users authenticate to the service?     | Workers sign in with a mobile telephone number and a single-use, time-limited code delivered by SMS. There is no worker password and no email address is required, which removes the two commonest frontline credential risks: shared passwords and password reuse. Sessions persist for up to 30 days so a worker is not asked for a code at every shift. Access is revoked automatically on a worker's recorded leaving date, including mid-session. Single sign-on and SCIM are <b>not</b> currently supported.                                                                                                                              |
| 31 What audit logging is in place?                   | Administrator actions, support impersonation, account creation and deletion, leaving-date changes, and publication and deletion of posts are all logged. Every support impersonation records the operator, the impersonated user, the tenant and the timestamp, and the log is available to you on request. Application and access logs are retained <u>[90]</u> days. <b>LOG RETENTION AND WHETHER THE IMPERSONATION LOG IS EXPORTABLE</b>                                                                                                                                                                                                     |
| 32 How is the service monitored?                     | External uptime monitoring at <u>[1 minute]</u> intervals and in-application error monitoring, both alerting an on-call engineer by <u>[email and SMS]</u> . <b>THE MONITORING TOOLS BY NAME; IF THE ERROR TOOL STORES REQUEST PAYLOADS IT IS A SUB-PROCESSOR AND MUST BE LISTED AS ONE</b>                                                                                                                                                                                                                                                                                                                                                     |
| 33 How do you manage patching and vulnerabilities?   | Unattended security updates are enabled on all servers. Updates for vulnerabilities the vendor rates critical or high, or carrying a CVSS v3 base score of 7 or above, are applied <b>within 14 days of release</b> , which is the Cyber Essentials requirement, and within <u>[72 hours]</u> where a vulnerability is being actively exploited. Dependencies are reviewed <u>[monthly]</u> with automated vulnerability alerting. Software is removed or upgraded before it reaches end of support.                                                                                                                                            |
| 34 When was your last penetration test?              | <u>[An independent external test was carried out by [supplier] on [date]. A summary report and the remediation status are available under a mutual non-disclosure agreement.]</u> If no test has been carried out, say so and give the planned date rather than leaving this blank; a scheduled date is a credible answer and an evasion is not. <b>WHETHER A TEST HAS BEEN DONE, BY WHOM, WHEN, AND THE REMEDIATION STATUS</b>                                                                                                                                                                                                                 |
| 35 Do you follow a secure development process?       | All changes go through source control and deploy from a protected branch. The framework provides protection against SQL injection, cross-site scripting and cross-site request forgery by default and those protections are not disabled. Dependencies are pinned and monitored for known vulnerabilities. Production personal data is not copied into development or staging environments.                                                                                                                                                                                                                                                     |
| 36 How is our data segregated from other customers'? | TeamTalk is multi-tenant. Each customer has 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. A user in one tenant cannot enumerate, read or address users, posts or files in another. Dedicated-database deployment is available for enterprise customers. <b>CONFIRM AUTOMATED TESTS ASSERT CROSS-TENANT ISOLATION, AND CITE THEM; THIS IS THE QUESTION A SECURITY REVIEWER ASKS TWICE</b> |

| QUESTION                                                | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 37 How are personnel vetted and trained?                | Right to work checks on all staff, written confidentiality obligations surviving the end of engagement, security and data protection briefing on joining and at least annually, and access removal on the last working day. <a href="#">[Basic DBS checks are obtained where a customer requires them.]</a> <b>STATE ONLY WHAT IS ACTUALLY DONE; DO NOT CLAIM BS 7858 SCREENING UNLESS IT HAS BEEN CARRIED OUT</b> |
| 38 How are end-user devices and remote working secured? | All laptops have full-disk encryption, an enabled software firewall, automatic operating system updates, malware protection and automatic screen lock. Company data is accessed only through the browser and the hosted tooling, not stored on the device where avoidable. Removable media is not used for customer data. Devices are in scope of the Cyber Essentials certification.                              |

#### D · Business continuity, backup and incident response (39 to 45)

| QUESTION                                                              | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 39 Do you have a business continuity and disaster recovery plan?      | Yes, a written one-page plan covering loss of the production environment, loss of a critical third-party service, loss of key personnel and loss of premises, reviewed <a href="#">[annually]</a> and after any incident. A summary is supplied as a separate document. <b>DATE OF THE LAST REVIEW</b>                                                                                                                                                                                                                                                                                                   |
| 40 What are your RTO and RPO?                                         | Recovery time objective <a href="#">[4]</a> hours for the application from a confirmed loss of the production server. Recovery point objective <a href="#">[24]</a> hours, or <a href="#">[5 minutes]</a> where point-in-time recovery is enabled on the managed database. <b>RTO AND RPO, AND EVIDENCE FROM A TIMED DRILL RATHER THAN AN ESTIMATE; THIS IS THE ANSWER PROCUREMENT MOST OFTEN FOLLOWS UP ON</b>                                                                                                                                                                                          |
| 41 How often is data backed up, and where is it held?                 | The database is backed up <a href="#">[daily]</a> , encrypted, and stored in Amazon S3 in the same UK region with versioning enabled. Uploaded files are held in S3, which is designed for high durability. Backups never leave the UK. <b>FREQUENCY, DESTINATION AND WHETHER FILES ARE SEPARATELY BACKED UP</b>                                                                                                                                                                                                                                                                                         |
| 42 How long are backups kept, and are restores tested?                | Backups are retained <a href="#">[30]</a> days and then deleted automatically. A full restore to a scratch environment is performed <a href="#">[quarterly]</a> , with the date, duration and outcome recorded. The most recent successful restore test was on <a href="#">[date]</a> . <b>RETENTION PERIOD AND THE DATE OF THE LAST SUCCESSFUL RESTORE TEST</b>                                                                                                                                                                                                                                         |
| 43 Do you have a documented incident response process?                | Yes, with a single named owner. It covers detection, containment, assessment, customer notification, remediation, and a written post-incident review. It is exercised <a href="#">[annually]</a> as a tabletop walkthrough. <b>DATE OF THE LAST EXERCISE</b>                                                                                                                                                                                                                                                                                                                                             |
| 44 How and when would you tell us about an incident?                  | By telephone and email to your named contact, without undue delay and in any event within 24 hours of becoming aware where personal data is involved, and within <a href="#">[24 hours]</a> for a security incident that does not involve personal data. You receive facts as they are confirmed, in phases if necessary, rather than a single late report.                                                                                                                                                                                                                                              |
| 45 What happens if you cease trading, or a key person is unavailable? | TeamTalk is a small company and says so. Credentials for all critical systems are held in <a href="#">[a password manager]</a> , with a documented emergency access arrangement held by <a href="#">[named person or the company's solicitor]</a> . On termination for any reason, including insolvency, your data is available for export in a machine-readable format for 30 days. Source code escrow is not offered as standard and would be considered for an enterprise agreement. <b>CONFIRM THE EMERGENCY ACCESS ARRANGEMENT EXISTS IN WRITING; PROCUREMENT ASKS THIS OF EVERY MICRO SUPPLIER</b> |

#### E · Sub-processors and supply chain (46 to 49)

| QUESTION                                                  | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 46 Who are your sub-processors?                           | Amazon Web Services (hosting, storage, backups, UK); Twilio (SMS sign-in codes, United States); OpenAI (translation of post text only, United States); Mux (video and captions, United States); Pusher (real-time delivery, optional and not used where self-hosted Reverb is deployed); <a href="#">[Mailgun or Amazon SES]</a> (transactional email); <a href="#">[error and uptime monitoring provider]</a> . The current list is published at <a href="https://team-comms.com/sub-processors">[https://team-comms.com/sub-processors]</a> . The list is deliberately short. |
| 47 How are we told about changes, and can we object?      | At least <b>30 days' written notice</b> before a new or replacement sub-processor begins processing, by email and by updating the published list. You may object on reasonable data protection grounds within 30 days. If TeamTalk cannot offer a reasonable alternative, you may terminate without penalty and receive a pro rata refund for the unexpired term.                                                                                                                                                                                                               |
| 48 What due diligence do you carry out on sub-processors? | Before engagement and at least annually: the provider's data processing terms and security documentation, its certifications, its data location, and its transfer mechanism, including verifying an active UK Extension certification on the Data Privacy Framework List where that route is relied on. Findings are recorded with a date.                                                                                                                                                                                                                                      |

| QUESTION                                                                 | ANSWER                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 49 Do your contracts with sub-processors flow down the same obligations? | Yes. Each is engaged under a written contract imposing the same data protection obligations as the customer agreement, as Article 28(4) of the UK GDPR requires. <b>Where a sub-processor fails to meet its obligations, TeamTalk remains fully liable to you for its performance.</b> Redacted terms are available on request. |

## F · Insurance (50 to 53)

| QUESTION                            | ANSWER                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 50 Professional indemnity insurance | £[limit] in the aggregate with [insurer], policy [number], renewing [date]. Certificate available on request. Note that many construction and facilities framework schedules require £5m maintained for six years after the end date. <b>THE LIMIT ACTUALLY HELD; DO NOT STATE A LIMIT YOU DO NOT HOLD, AND BUY THE LIMIT THAT CLEARS YOUR TARGET BUYERS BEFORE YOU NEED IT</b>                      |
| 51 Public liability insurance       | £[limit] per occurrence with [insurer], policy [number]. TeamTalk has no site presence and no operatives, so a lower public liability limit is frequently agreed for a pure software supplier. Ask. <b>THE LIMIT ACTUALLY HELD</b>                                                                                                                                                                   |
| 52 Employers' liability insurance   | [£10m with [insurer], policy [number]]. The statutory minimum under the Employers' Liability (Compulsory Insurance) Regulations 1998 is £5m; most insurers write £10m. If TeamTalk currently employs only its owner, who holds 50% or more of the issued share capital, the HSE treats it as exempt: say that plainly rather than leaving the field blank. <b>WHETHER COVER IS REQUIRED AND HELD</b> |
| 53 Cyber liability insurance        | £[limit] with [insurer], policy [number], including data breach response costs. <b>THE LIMIT ACTUALLY HELD, AND CHECK IT EXCEEDS ANY LIABILITY SUPER-CAP AGREED IN A CONTRACT</b>                                                                                                                                                                                                                    |

## G · Modern slavery, ethics and equality (54 to 56)

| QUESTION                                                   | ANSWER                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 54 Do you have a modern slavery statement?                 | Yes, published voluntarily. TeamTalk's turnover is below the £36 million threshold at which section 54 of the Modern Slavery Act 2015 requires a statement, so it is not legally obliged to publish one, and the statement says so. A one-page statement is attached and is published at [URL].                                                                   |
| 55 Do you have an anti-bribery policy?                     | Yes. TeamTalk is a relevant commercial organisation for the purposes of section 7 of the Bribery Act 2010, which has no size threshold, and maintains procedures proportionate to its risk in line with the Ministry of Justice statutory guidance. A one-page policy is attached. No director or employee has been convicted of a bribery or corruption offence. |
| 56 Do you have an equal opportunities or diversity policy? | Yes, a one-page policy covering the nine protected characteristics in section 4 of the Equality Act 2010. TeamTalk has not been the subject of any Equality and Human Rights Commission investigation or any finding of unlawful discrimination. The public sector equality duty does not apply to TeamTalk, which does not exercise public functions.            |

## H · Health and safety (57 to 58)

| QUESTION                                                   | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 57 Do you have a health and safety policy?                 | Yes. TeamTalk employs fewer than five people, so it is excepted from the duty in section 2(3) of the Health and Safety at Work etc. Act 1974 to prepare a written policy, by the Employers' Health and Safety Policy Statements (Exception) Regulations 1975. A written policy is maintained anyway and is attached. TeamTalk is a desk-based business: the material risks are display screen equipment, electrical safety and lone or home working, all assessed and recorded. <b>ONCE HEADCOUNT REACHES FIVE, THE WRITTEN POLICY BECOMES A LEGAL REQUIREMENT</b> |
| 58 Accident record, RIDDOR reports and enforcement history | No reportable incidents under RIDDOR 2013 in the last [three] years, no enforcement notices, and no prosecutions. TeamTalk personnel do not carry out work on customer premises. Where a visit to a site is arranged, TeamTalk personnel comply with the site induction and site rules and are escorted at all times. <b>CONFIRM THE ACCIDENT RECORD BEFORE ANSWERING</b>                                                                                                                                                                                          |

## I · Environment (59 to 60)

| QUESTION                                                        | ANSWER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>59 Do you have an environmental policy or ISO 14001?</b>     | A one-page environmental policy is maintained and attached. TeamTalk is not certified to ISO 14001 and does not claim to be. It is below the thresholds for Streamlined Energy and Carbon Reporting and for the Energy Savings Opportunity Scheme, and, as a micro business, the workplace recycling separation duty applies to it from 31 March 2027.                                                                                                                                                                                                         |
| <b>60 What is your carbon reduction or net zero commitment?</b> | TeamTalk is a remote-first software business with no premises-based operations, no fleet and no manufacturing, so its direct emissions are minimal and its principal impact is the energy used by its cloud hosting. It hosts on AWS in the eu-west-2 region, and AWS publishes its own renewable energy commitments. <a href="#">[A carbon reduction plan to PPN 006 format is available where a customer requires one.]</a> <b>WHETHER A CARBON REDUCTION PLAN IS NEEDED; CENTRAL GOVERNMENT CONTRACTS ABOVE £5M REQUIRE ONE, MOST PRIVATE BUYERS DO NOT</b> |

### Every [verify] value in one list

Confirm these once, write them into this document, and the next questionnaire takes an hour. Ranked by how often a buyer follows up on the answer.

| VALUE                                                                | QUESTION   | HOW TO CONFIRM IT                                                       |
|----------------------------------------------------------------------|------------|-------------------------------------------------------------------------|
| Recovery time and recovery point objectives                          | 40         | Run a timed restore drill and record the elapsed time. Do not estimate. |
| Backup frequency, destination and retention                          | 19, 41, 42 | Read it off the backup configuration, not from memory.                  |
| Date of the last successful restore test                             | 42         | Do one this month if there is no date to give.                          |
| Penetration test: whether, by whom, when                             | 34         | If none, book one or give the planned date.                             |
| Cyber Essentials certificate number and expiry                       | 23         | From the IASME certificate.                                             |
| Insurance limits actually held                                       | 50 to 53   | From the schedules. Never state a limit not in force.                   |
| ICO registration number and renewal date                             | 9          | From the ICO register entry.                                            |
| Hosting region for this deployment                                   | 16         | From the AWS console.                                                   |
| Cross-tenant isolation test coverage                                 | 36         | Cite the tests by name; write them if they do not exist.                |
| Monitoring tool names, and whether the error tool is a sub-processor | 32, 46     | Check whether it stores request payloads.                               |
| Number of people with production access, last review date            | 27         | From the access review record.                                          |
| Log and impersonation log retention                                  | 31         | From the log rotation configuration.                                    |
| Turnover, headcount and VAT position                                 | 3, 5, 6    | From the filed accounts and payroll.                                    |
| Emergency access arrangement for credentials                         | 45         | Write it down and tell the named holder.                                |
| Personnel vetting actually carried out                               | 37         | State only what is done.                                                |
| Accident and enforcement record                                      | 58         | Check before asserting a nil return.                                    |

**Not legal advice.** These are drafting aids, not warranties. Every answer becomes a contractual representation once it is in a completed questionnaire, so confirm each one before sending. **Sources, verified 28 August 2026:** UK GDPR Articles 28, 30, 32, 33 and 37, 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 [legislation.gov.uk/ukpga/2025/18](#); ICO data protection fee, tier 1 £52, or £47 by direct debit, under SI 2018/480 as amended by SI 2025/63 [ico.org.uk/data-protection-fee](#); ICO transfer tools, IDTA version A1.0 and Addendum version B1.0, in force 21 March 2022 [ico.org.uk/international-transfers](#); Data Protection (Adequacy) (United States of America) Regulations 2023, SI 2023/1028 [legislation.gov.uk/uksi/2023/1028](#); NCSC Cyber Essentials: Requirements for IT Infrastructure v3.3 [ncsc.gov.uk/cyberessentials](#); Modern Slavery Act 2015 s.54 and SI 2015/1833 reg. 2 (£36m threshold) [legislation.gov.uk/ukpga/2015/30/section/54](#); Bribery Act 2010 s.7 [legislation.gov.uk/ukpga/2010/23/section/7](#); Equality Act 2010 s.4 [legislation.gov.uk/ukpga/2010/15/section/4](#); Health and Safety at Work etc. Act 1974 s.2(3) and SI 1975/1584 reg. 2 [legislation.gov.uk/uksi/1975/1584](#); Employers' Liability (Compulsory Insurance) Regulations 1998, SI 1998/2573 reg. 3(1), and HSE leaflet HSE40 [hse.gov.uk/pubns/hse40.pdf](#); RIDDOR 2013, SI 2013/1471 [legislation.gov.uk/uksi/2013/1471](#); Simpler Recycling micro-firm date, SI 2025/140 reg. 4 [legislation.gov.uk/uksi/2025/140](#).