Gatherwell

Security questionnaire for accounting firms

Answered in advance so that your security review is a link rather than an afternoon. Short-form, in the shape of a SIG Lite. If your review needs a question that is not answered here, ask and we will answer it in writing and add it to this document.

Gatherwell, client document chasing for accounting firms. Completed September 2026.

Answers marked 'in progress' are stated as such rather than implied to be in place.

Scope and summary

Gatherwell collects accounting records from an accounting firm's clients. The firm creates a request from a template; the client receives a link with a checklist and either uploads the documents or replies to the email with them attached; the system chases every outstanding item until the pack is complete. The firm is the data controller and Gatherwell is the processor.

> The short version for a reviewer in a hurry: data is held in the EU, encrypted in transit and at rest, isolated per firm at two layers with an automated test that must pass before any deployment, scanned for malware on arrival, deleted on a schedule the firm sets, and covered by a signed data processing agreement. We do not hold ISO 27001. Cyber Essentials is in progress. We would rather say so than imply otherwise.

A. Company and scope

Question	Answer
A1. Legal entity and location	Gatherwell, United Kingdom. Working product name; the contracting entity is confirmed at contract.
A2. What the service does	Collects and chases client documents for accounting, bookkeeping and tax practices.
A3. Who the data subjects are	The firm's clients and their contacts, and the firm's own staff.
A4. Data processed	Names, email addresses, mobile numbers, and the contents of documents clients send: bank statements, invoices, receipts, payslips, tax documents, and identification documents where the firm requests them.
A5. Special category data	Not requested by any template. It can appear incidentally inside an uploaded document and is handled with the same controls as everything else.
A6. Sub-contracting	Sub-processors are listed at document.yarqat.com/security. Thirty days' notice before any addition, with a right to object.

B. Hosting and data location

Question	Answer
B1. Where is data hosted	European Union. Application servers, database, object storage and backups are all EU region. A UK region option is available on request.
B2. Are there transfers outside the EU or UK	No. If a sub-processor ever required one we would rely on an adequacy decision or standard contractual clauses with a transfer risk assessment, and would notify the firm first.
B3. Physical security	Inherited from the hosting provider's certified data centres. Gatherwell staff have no physical access to hardware.
B4. Tenancy model	Multi-tenant, logically isolated. See section D.

C. Encryption

Question	Answer
C1. In transit	TLS 1.2 or better on every connection, including the client checklist page, the firm application, the inbound email endpoint and all sub-processor calls. HTTP is redirected to HTTPS; HSTS is set.
C2. At rest	AES-256 on database volumes, object storage and backups.

Question	Answer
C3. Key management	Application keys are held outside the database and outside the source repository, in environment configuration readable only by the service account.
C4. Integration credentials	OAuth tokens for a firm's Google Drive or OneDrive are encrypted at the application layer and decrypted only inside the job that uses them. Never logged, never displayed, never returned by any interface.

D. Access control and isolation

Question	Answer
D1. How is one firm's data kept from another's	Two layers. Every tenant model carries a firm scope applied globally at the application layer, and PostgreSQL row-level security enforces the same rule in the database, so a query that forgets the filter returns nothing rather than another firm's records.
D2. Is that tested	Yes. An automated test logs in as one firm and attempts to read another firm's records through every route and every endpoint. It must pass before any deployment.
D3. Authentication	Two-factor authentication is mandatory for firm owners and available to all staff. Sessions expire after eight hours. Login is rate limited.
D4. Client access	Clients never create an account. A checklist link carries a 128-bit random token, expires 30 days after the request completes, is bound to the first device that opens it, and requires an emailed code on a new device. A PIN can also be required.
D5. Internal access	Least privilege, individually named accounts, no shared logins. Production access is logged.
D6. Audit logging	Append-only log of every change to a request and every file access, recording actor, action and time. Exportable by the firm. Not alterable after the fact.

E. Handling of files received

Question	Answer
E1. Malware scanning	Every inbound file is scanned before it is stored.
E2. File type handling	Type is checked against content rather than extension. Images are re-encoded. Size limits are enforced. Files are never executed.
E3. Serving files back	Only through short-lived signed links.
E4. Raw email retention	Raw inbound email is kept 30 days so a failed delivery can be reprocessed, then purged.
E5. Logging of content	File contents and message bodies are excluded from application logs and from error reports by configuration.

F. Retention, deletion and portability

Question	Answer
F1. Retention	Set by the firm. Files are deleted when the period expires.
F2. Export	The firm can export everything at any time, without asking us: JSON plus the files as a zip.

Question	Answer
F3. Deletion on termination	Recoverable for 30 days, then permanently deleted. The deletion is recorded in the audit log and a certificate is available on request.
F4. Backups	Nightly database dump with continuous write-ahead log archiving to EU storage. Backups age out within 35 days. A deleted firm is not restored from backup.
F5. Restore testing	A scripted restore into a scratch database with a row count check, run weekly by cron.

G. Resilience and operations

Question	Answer
G1. Availability target	99.5 percent monthly outside announced maintenance.
G2. Maintenance	Announced at least 48 hours ahead, scheduled outside UK business hours where possible.
G3. Deployment	Zero-downtime releases with a one-command rollback. Automated tests, including the tenancy isolation test, must pass first.
G4. Monitoring	Error tracking and uptime monitoring on the application and the inbound email endpoint. A daily reconciliation job compares inbound messages received against submissions created and alerts on any mismatch.
G5. Environments	Separate local, staging and production. Production data is not copied into staging.

H. Incident response

Question	Answer
H1. Acknowledgement	Within four working hours of detection or report.
H2. Containment	Containment before diagnosis: roll back, disable the feature flag, or pause the job.
H3. Notification to the firm	Without undue delay and within 72 hours of becoming aware of a personal data breach affecting the firm's data, in line with UK GDPR, saying what happened, what we changed and what to watch.
H4. Post-incident	A written note within 24 hours of resolution: cause, change made, what is now monitored. Blameless and specific.
H5. Responsible disclosure	Reports are welcome and are answered by a person. We do not take legal action against good-faith reporters.

I. Governance, assurance and insurance

Question	Answer
I1. UK GDPR and EU GDPR	In place. Data processing agreement published at document.yarqat.com/dpa and signable before any data is sent.
I2. Cyber Essentials	In progress. The certificate will be published on the security page when issued.
I3. ISO 27001	Not held, and not claimed.
I4. SOC 2	Not held, and not claimed.
I5. Penetration testing	An external review of link handling and firm isolation is planned before the full launch. Not yet completed.

Question	Answer
I6. Professional indemnity and cyber insurance	In progress; details will be added here when the policy is in force.
I7. Staff	Small team. Everyone with access is bound by confidentiality terms and access is removed on the day someone leaves.
I8. Artificial intelligence	None in the product today. When document classification arrives it will be opt-in per firm, with no training on customer data, prompts logged without file content, and account numbers redacted before anything is sent to a model.

J. What we are not

Stated plainly, because a questionnaire that answers every question with a yes is not worth reading. Gatherwell is a small supplier. We do not hold ISO 27001 or SOC 2, we have not yet completed a penetration test, and Cyber Essentials is an application rather than a certificate. What we do have is a narrow product, data in the EU, isolation enforced at two layers and tested on every deployment, deletion you control, and a named UK practising accountant on the team who will take your call. If that is not enough for your review, say so and we will tell you honestly whether we can close the gap or not.

Contact for security questions and incident reports: through document.yarqat.com, marked security. Answered by a person. This document is reissued whenever an answer changes.