Supplier Risk Management Policy

1. Purpose

This policy sets out how Subcontext selects, contracts with and monitors the suppliers and sub-processors that the platform depends on, so that the risks they bring are understood and controlled.

Our customers are regulated firms who outsource part of their services to us. Under FCA SYSC 8 and PRA Supervisory Statement SS2/21, they remain responsible for the services they outsource, including where we in turn rely on our own suppliers. This policy explains how we manage that chain so that customers can rely on it.

2. Scope

It covers every supplier that processes customer data, supports the running of the platform, or could affect its security or availability. The current sub-processors are published in the Sub-Processor List.

It applies across the whole supplier lifecycle: identifying the need, due diligence, contracting, onboarding, ongoing monitoring, and offboarding.

3. Definitions

Term	Meaning
Supplier	Any third party that provides goods or services to Subcontext
Sub-processor	A supplier that processes personal data on behalf of Subcontext's customers
Supplier register	Subcontext's record of its suppliers, their tier, the data they process and their review dates
Material supplier	A Critical supplier, or any supplier whose failure would stop or seriously degrade a service customers rely on

4. Roles and Responsibilities

Role	Responsibility
Directors	Approve this policy, approve the engagement of every Critical supplier, and accept any residual risk that cannot be reduced
Security Officer (a member of the founding team)	Owns this policy and the supplier register, carries out or reviews due diligence, and tracks reviews and actions
Person engaging the supplier	Identifies the need, gathers the information needed for due diligence, and does not share customer data until the supplier is approved

5. Supplier Tiers

Tier	Description	Examples
Critical	Processes customer personal data, or the platform cannot run without it	AWS, AWS Bedrock, Twilio, Stripe, OpenAI, Meta
High	Processes customer data for specific features	ElevenLabs, Data8, Iress, Google
Standard	No access to customer data	Professional services, productivity tools

A supplier's tier is set when it is first assessed, and reassessed whenever the way we use it changes. If a supplier could fit more than one tier, the higher tier applies.

6. Due Diligence Before Engagement

Before a Critical or High supplier is engaged, we assess:

- Security assurance, such as ISO 27001 certification or SOC 2 reports
- Data protection terms meeting Article 28 of the UK GDPR
- Where data is stored and processed, and the transfer safeguards in place
- For AI providers: whether customer data is retained, and confirmation that it is not used to train models
- Financial standing and service resilience

We also consider:

- What customer data the supplier would receive, and whether less could be sent
- How the supplier would notify us of incidents and service disruption
- Whether we could replace the supplier, and how long that would take
- Concentration risk, where we already rely on the same supplier for other services
- For transfers outside the UK, a transfer risk assessment, as described in the Transfer Risk Assessment

Standard suppliers are checked in proportion to the risk, for example confirming they will not receive customer data.

6.1 Approval procedure

1. The person engaging the supplier records the need, the proposed tier and the data involved.
2. The Security Officer completes the due diligence above and records the findings and any risks.
3. Critical suppliers are approved by the directors. High suppliers are approved by the Security Officer. Standard suppliers are approved by the person engaging them.
4. The supplier is added to the supplier register before any customer data is shared with it.
5. New sub-processors are added to the Sub-Processor List and customers are notified, as described in section 10.

6.2 Worked example

A speech synthesis supplier for phone conversations would receive the text of agent replies, which may include personal data. That places it in the High tier. Due diligence covers its security assurance, its data processing terms, where it processes data (if in the US, transfer safeguards are required) and whether it

retains or trains on customer data. Once approved, it is added to the supplier register and the Sub-Processor List before any customer data is sent to it.

7. Contractual Requirements

Agreements with suppliers that process customer data include:

- Data processing terms, confidentiality and security obligations
- Prompt notification of personal data breaches
- Flow-down of equivalent obligations to their own sub-processors
- Audit rights, or access to independent assurance reports

Where possible, we also look for:

- Commitments on service availability and support
- Notice of material changes to the service, or to the supplier's own sub-processors
- Return or deletion of our data at the end of the contract
- Termination rights that allow us to move to another supplier in an orderly way

Many of our suppliers are large providers that contract on standard terms. Where we cannot negotiate terms, we assess the standard terms against these requirements and record any gaps and how we manage them.

8. Technical Safeguards

- Only the data a supplier needs for its task is sent to it
- AI inference is pinned to UK and EU regions: requests to US-routed models are refused
- Each customer's messaging runs in its own isolated Twilio account where enabled
- Credentials for suppliers and customer integrations are encrypted at rest
- Callbacks from suppliers (payments, messaging, email) are signature-verified and rejected if the signature fails

In addition, payment card details are handled by Stripe and are never stored by Subcontext. AWS Bedrock does not store or train on prompts and responses. For voice, OpenAI does not train on API data, though it may keep data for up to 30 days for abuse monitoring.

9. Ongoing Monitoring

- Critical suppliers are reviewed at least annually, High suppliers every two years
- Supplier status and security advisories are monitored
- A supplier register records each supplier, its tier, the data it processes and its review date

A review checks that the supplier's assurance is still current, that its terms still meet section 7, that any incidents or service problems have been addressed, and that its tier is still right. A supplier is also reviewed straight away if it suffers a significant security incident or outage, changes ownership, or changes where it processes data.

Supplier incidents that affect customers are handled under the Incident Response Plan.

10. Changes to Sub-Processors

New sub-processors are added to the published Sub-Processor List, and customers are notified in accordance with the Data Processing Agreement.

11. Exit and Contingency for Material Suppliers

For each material supplier, we keep a note of how we would continue if it failed or had to be replaced. Some of these arrangements already exist in the platform:

Supplier type	Contingency
AI model provider	Agents can be moved to an alternative model
Messaging or telephony	Conversations continue on unaffected channels while the provider recovers
Payments	Payment steps are paused and resumed when the provider recovers
Hosting	Infrastructure is defined as code, so the environment can be rebuilt

See the Operational Resilience Statement for how these scenarios are handled.

12. Offboarding

When a supplier is replaced or no longer needed, its access is revoked, credentials are rotated, and deletion or return of our data is confirmed.

The supplier register and, where relevant, the Sub-Processor List are updated once offboarding is complete.

13. Exceptions

An exception to this policy, for example engaging a supplier before its due diligence is complete, needs a written reason, a risk assessment by the Security Officer, and director approval. Customer data is not shared with a supplier under an exception unless the directors have accepted the risk in writing. Exceptions are time-limited and reviewed at the next supplier review.

14. Compliance

The Security Officer checks at least annually that every supplier in use is on the supplier register, that its tier is right, and that its reviews are up to date. The results are reported to the directors.

15. Related Documents

- Sub-Processor List
- Transfer Risk Assessment
- Information Security Policy
- Operational Resilience Statement
- Incident Response Plan
- Exit Plan & Data Return Policy

- Data Protection Impact Assessment

16. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and when a new Critical supplier is engaged
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.