Service Levels & Support Policy

1. Purpose

This policy sets out the availability we aim for, how customers get support, and how quickly we respond.

It is intended to give customers, including their procurement and outsourcing teams, a clear view of the service they can expect, so they can reflect it in their own service management, outsourcing records and operational resilience mapping.

2. Scope

This policy applies to the Subcontext platform: the dashboard, AI agents on every channel, the REST API, the MCP server, embedded widgets, and the iOS, Android and Mac apps. Specific terms agreed in a customer's order form take precedence over this policy where they differ.

3. Definitions

Term	Meaning
Business hours	09:00 to 17:30 UK time, Monday to Friday, excluding public holidays in England
Business day	A day on which business hours apply
Availability	The proportion of a calendar month in which the platform is available for customers to use, excluding the exclusions in section 4
First response	A reply from a member of the Subcontext team that acknowledges the request and either answers it or explains the next step. Automatic acknowledgements do not count
Incident	An unplanned interruption to, or reduction in the quality of, the platform, or a suspected or actual security breach

4. Availability

- We target 99.9% monthly availability for the Subcontext platform
- Planned maintenance is excluded, and announced in advance where practicable
- Most releases are deployed without downtime
- Outages at third-party providers outside our control (for example a messaging network) can affect individual channels; we tell affected customers and keep unaffected channels running
- Enterprise customers may agree service credits in their order form

4.1 What 99.9% means in practice

Period	Maximum unplanned unavailability at 99.9%
30-day month	About 43 minutes
Year	About 8 hours 46 minutes

4.2 How availability is supported

The platform runs in the AWS EU (Ireland) region, with application servers spread across two availability zones. Servers scale automatically with demand, and unhealthy servers are replaced automatically. Releases are rolled out gradually, so most are deployed without interrupting customers. See the Operational Resilience Statement for more detail and our recovery objectives.

4.3 Planned maintenance

Where maintenance needs downtime, we aim to schedule it outside UK business hours and tell customers in advance by email. A holding page is shown while it runs. Urgent maintenance needed to protect the security or integrity of the platform may happen at short notice.

5. How to Get Support

- **In the dashboard:** open a support ticket from Help, and follow its progress there
- **By email:** support@subcontext.com
- Ticket replies arrive by email, and you can reply to them directly

To help us respond quickly, please include:

- Your organisation name, and the user affected
- What you were trying to do, what happened, and when
- Any reference such as a conversation, lead, application or policy, and screenshots where useful
- How many people or customers are affected, and whether there is a workaround

Please do not send passwords, full card numbers or other secrets in a support request. We will never ask for your password.

6. Support Hours

Monday to Friday, 09:00 to 17:30 UK time.

Incidents are handled outside these hours where needed, as set out in section 8.

7. First Response Targets

Plan	First response
Enterprise	Within 4 business hours
Professional	Within 1 business day
Starter and other plans	Within 2 business days

Response targets are measured from when the request is received during business hours. A request received outside business hours is treated as received at the start of the next business day.

Worked example

A Professional customer emails support at 16:45 on a Friday. The first response target is 1 business day, so a reply is due by 16:45 on Monday. An Enterprise customer raising the same request would get a reply by 12:15 on Monday (45 minutes on Friday and 3 hours 15 minutes on Monday).

8. Incidents

Incidents affecting the platform are handled under the Incident Response Plan, outside support hours where needed:

Severity	Example	Response
Critical	Platform unavailable, or a data breach	Within 1 hour
High	A major feature or channel unavailable	Within 4 hours
Medium	A feature degraded, with a workaround	Within 1 business day
Low	A minor issue or question	Within the plan's first response target

Subcontext decides the severity of an incident, taking account of the impact the customer reports. If a customer thinks the severity is wrong, they can say so in the ticket and we will review it. Severity can go up or down as we learn more.

8.1 How we detect incidents

Application errors and performance are monitored continuously. Infrastructure alarms cover the database, cache, load balancer and application servers, and alert the team by email. Customers can also report a suspected incident through support at any time.

8.2 Response and resolution

The response time is the time within which we start working on the incident. Resolution depends on the cause. Where a full fix will take time, we aim first to restore service or provide a workaround, and then fix the underlying cause.

9. Communication

Customers affected by an incident are told by email, with updates until it is resolved and a summary afterwards for Critical incidents.

The summary sets out what happened, when, which services and customers were affected, the cause, and what we are doing to stop it happening again. Where an incident involves personal data, we also notify the customer in line with the Data Processing Agreement and the Incident Response Plan.

10. Customer Responsibilities

To get the best from support and the platform, customers:

- Keep the contact details for their organisation's owners up to date, so incident notices reach the right people
- Report problems promptly, with the information listed in section 5
- Keep fallback arrangements for services that depend on Subcontext, such as handing conversations to their own team

11. Escalation

If a support request is not progressing as expected, reply to the ticket and ask for it to be escalated. It will be reviewed by a member of the founding team. If you are unhappy with the service you have received, you can also make a complaint under the Complaints Handling Policy.

12. Measuring and Reviewing Performance

We track first response times against the targets in section 7, and record incidents and their causes. These are reviewed at least quarterly to find recurring problems and improve the service. Enterprise customers can ask for a summary of their support and incident history.

13. Related Documents

- Incident Response Plan
- Operational Resilience Statement
- Business Continuity & Disaster Recovery Policy
- Change Management Policy
- Complaints Handling Policy

14. Document Control

Item	Detail
Owner	A director of Subcontext Ltd
Approved by	The directors of Subcontext Ltd
Review	At least annually
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.