Schedule 4 — Support Policy

ATSC Global Limited · how incidents are logged, classified, escalated and resolved

Field	Detail
Document reference	ATSC-SCH4-SUP
Version	1.0, November 2026
Effective date	[DATE OF PUBLICATION]
Read with	Schedule 3 (Service Level Agreement), which sets availability and service credits

1. Definitions

1.1 Capitalised terms not defined here have the meaning given in Schedule 1 (Definitions). In this Schedule:

"Incident" means an unplanned interruption to, or reduction in the quality of, a Service, or a failure of a Service to perform materially in accordance with its Documentation.

"Response" means the Supplier's acknowledgement of an Incident by a qualified engineer who has begun work on it, as distinct from an automated ticket receipt.

"Workaround" means a temporary solution that restores the affected function, or reduces the Incident's impact so that it qualifies for a lower Severity.

"Resolution" means a permanent fix, or a Workaround accepted by the Customer acting reasonably, after which the Incident no longer meets its Severity definition.

"Support Hours" means Business Hours in the Customer's operating time zone recorded in the Works Order. Support outside Business Hours is provided only where a Works Order expressly provides for it.

2. Support tiers

2.1 The Customer provides first-line support to its Authorised Users and End Users: receiving reports, answering how-to questions, and triaging before escalation. The Customer shall nominate up to three (3) trained contacts who may log Incidents with the Supplier, or such other number as the Works Order states.

2.2 The Supplier provides second-line support (diagnosis and resolution of Incidents in the Service) and third-line support (code-level fixes, platform engineering and vendor escalation). The Supplier may perform support through its Affiliates and through Sudo Sky Limited.

2.3 Support for Customer-built extensions, custom code, third-party integrations not supplied by the Supplier, or the Customer's own infrastructure is outside this policy and is chargeable as professional services.

3. Severity, response and resolution

3.1 The Customer proposes a Severity when logging an Incident. The Supplier confirms or adjusts it in consultation with the Customer, acting reasonably. If the Customer does not propose a Severity, Severity 3 applies until confirmed.

Severity	Definition	Support Hours	Response	Update interval	Resolution target
1 — Critical	A production Service is unavailable, or a core function is unusable for all or most users, or there is a confirmed security incident affecting Customer Data. No Workaround.	Support Hours	1 Business Hour	Every 2 Business Hours, until a Workaround is in place	Workaround within 4 Business Hours; Resolution worked continuously during Support Hours
2 — High	A core function is seriously degraded or unavailable for a group of users, with material business impact. No reasonable Workaround.	Support Hours	2 Business Hours	Every Business Day	1 Business Day
3 — Medium	A non-core function is impaired, or a core function is affected for individual users, or a reasonable Workaround exists.	Support Hours	8 Business Hours	Every 5 Business Days	10 Business Days
4 — Low	A cosmetic issue, documentation error, question, or request for enhancement.	Support Hours	2 Business Days	On status change	Next scheduled release, or as agreed

3.2 Resolution targets are targets, not guarantees. A failure to meet a Resolution target is not of itself a breach of the Agreement. The Customer's remedies for unavailability are the Service Credits and chronic failure right in the SLA. For Severity 1 Incidents the Supplier shall provide a root-cause analysis in accordance with the SLA.

3.3 Incidents of any Severity logged outside Support Hours are treated as received at the start of the next Support Hours period. Resolution targets do not apply during an agreed onboarding or implementation period before the Customer signs acceptance under the Works Order.

4. How to log an Incident

4.1 Incidents are logged through the support portal at atsc.global/support or by email to support@atsc.global. Severity 1 Incidents must be logged through the support portal, or by email with "Severity 1" in the subject line, so that they are prioritised.

4.2 The Customer shall provide the information reasonably needed to reproduce and diagnose the Incident: the Service and environment affected, the time of occurrence, steps to reproduce, the number of users affected, error messages, and screenshots or logs where available. Response and update clocks start when the Supplier receives that information.

5. Escalation

5.1 If an Incident is not progressing in line with this policy, the Customer may escalate it to the next level:

Level	Role	Contact	Escalate after (Severity 1 / 2 / 3 / 4)
1	Support Desk	support@atsc.global	On logging
2	Support Manager	support-escalation@atsc.global	2 hours / 4 hours / 3 Business Days / 10 Business Days
3	Head of Operations	operations@atsc.global	4 hours / 1 Business Day / 7 Business Days / not applicable
4	Director	legal@atsc.global	8 hours / 2 Business Days / not applicable / not applicable

6. Support allocations and charges

6.1 Where a Works Order includes an allocation of support hours, time spent on Incidents caused by a defect in the Service, an outage of the Supplier's hosting environment, or a security incident in the Supplier's systems does not count against the allocation.

6.2 Support for matters excluded by paragraph 2.3, and support in excess of an allocation, is charged at the rates in the Works Order.

7. Maintenance and releases

7.1 Scheduled Maintenance is governed by the SLA. The Supplier shall publish release notes for each Upgrade, and shall give at least thirty (30) days' notice of any change that removes or materially changes a feature or published interface, in accordance with clause 16 of the Agreement.

7.2 The Supplier supports the current major release of each Service and the release before it. Where a Service is deployed on the Customer's infrastructure, the Customer shall install Updates that address security vulnerabilities within thirty (30) days of release, or within seven (7) days for vulnerabilities the Supplier designates as critical.

8. Customer obligations

8.1 The Customer shall: maintain trained first-line contacts; give the Supplier remote access to affected environments where needed, subject to the Customer's security rules notified in advance; implement Workarounds and Updates the Supplier provides; and keep its own systems and integrations within the supported configurations in the Documentation.

End of Schedule 4.