

Service Operations & Support Pack

A practical operating model for receiving cases, restoring service, communicating clearly and learning from customer experience.

Version 0.1-public | Public reference draft | JEL Project Management

Purpose and activation boundary

This pack consolidates the existing support drafts and links them to the published sales/pilot/onboarding process. It defines how the service should operate; it does not configure a service desk, establish a staffed roster, appoint a provider, change a customer contract or activate an SLA.

The minimum service to put in place

One tested intake route; one accountable case owner and a real backup; an approved support calendar and target set; a reliable escalation route; and evidence that a second person can execute the handover and incident procedure.

Use this pack	Pages
Ownership, support scope and service-level decisions	2-5
Case handling, major incidents and AIDE Ops visibility	6-8
Troubleshooting, release and recovery controls	9-10
Readiness rehearsal, handover and operating measures	11-12
Approval register and source/evidence boundaries	13-14

Companion documents

The editable Templates & Checklists contains the service schedule, roster, case/escalation record, incident/review record, customer communications, handover and rehearsal forms. Customer Support Overview is a separate public-safe draft; approved customer service schedules remain separate from this public reference draft.

Three distinctions that must remain visible

Published targets are not the same as older proposed targets. Repository capability is not proof of a deployed, monitored service. A green heartbeat is not proof that customer usage or integration evidence is complete and fresh.

1. Ownership and support levels

Keep the customer-facing case owned while technical work moves between teams.

Role	Responsibility and boundary
Accountable service owner	Approve scope, coverage, staffing, risk exceptions and service schedules. Nominate a deputy and ensure coverage during absence. The accountable owner, acceptance and deputy must be recorded.
L1 - Customer support	Validate customer/contact, gather evidence, triage, apply approved how-to/access procedures and maintain customer updates. Do not change billing, privileges or production infrastructure without authority.
L2 - Product support	Investigate product behaviour, integrations and configuration; reproduce safely; identify workarounds; raise linked engineering work.
L3 - Engineering & platform	Own code, database/platform diagnosis, release/recovery execution and complex defects. Production changes require the authorised change path.
Incident / security lead	For a major incident, coordinate technical work, impact assessment and communications. Security lead restricts evidence and coordinates notification assessment.
Customer Owner / technical lead	Approve customer access or configuration changes; validate business impact, source-system permissions and service recovery.

Partner arrangement: confirm, do not presume

A support provider must be explicitly appointed; this pack does not evidence an executed support agreement or staffed coverage. Name the actual provider, individuals, backup, escalation contacts, access permissions and operating obligations in template T2 before allocating live cases.

Handover and absence

At the end of each covered shift, explicitly transfer active incidents, imminent deadlines and unowned cases to an accepting person. Do not allow a mailbox or queue name to substitute for an accountable owner. Where roles are combined in a small team, preserve separate change authorisation and customer communication decisions.

Access boundary

Use named accounts, least privilege and approved customer scope. Domain matching can suggest a customer; it does not prove identity or authorise disclosure. Verify privileged requests against the established customer contact record. Never share credentials to cover staff absence.

2. Service scope and intake

Support the licensed product; keep new delivery work and consulting explicitly scoped.

Included within agreed support	Separate or customer-owned work
Account access, MFA/recovery and role troubleshooting	A request to grant privilege still needs customer authority; troubleshooting is not approval.
AIDE Chain / Blueprint incidents, defects and standard configuration guidance	New functionality, unsupported connectors, architecture consulting or project-management consulting require separate approval/scope.
Supported integration diagnosis on the AIDE side	Customer source-system, network or supplier faults remain with their owner. AIDE still coordinates and communicates its own case.
Subscription and entitlement fault investigation	Refunds, seat purchases, contract changes and paid activation require authorised commercial approval.
Platform incident coordination and agreed recovery support	Bulk data remediation, bespoke migrations or new deployments outside the accepted scope are separate work.

Primary and fallback channels

The earlier draft proposes a support mailbox and a customer portal once connected/configured. That is not evidence that email-to-case, reply threading or a staffed portal is currently working. Confirm the real monitored route with an external round-trip test before announcing it. [S1-S2]

Jira Service Management was the recommended case platform in the earlier procedure. A partner ITSM platform is another candidate only if it meets the same controls and an agreement is reached. Select one authoritative case record; AIDE Ops is not a substitute for that record.

If the service desk or sign-in is unavailable

Record a fallback contact route independent of product sign-in and, where practicable, of the failed service. Test that route with the named backup. During an intake outage, use an approved restricted manual register with original receipt times; reconcile entries into the service desk after recovery. Never backdate the first response or lose the original clock.

Customer submissions and security reports

Request organisation, affected environment, impact, start time/time zone, module and safe reproduction detail. Accept suspected security reports from any reporter without granting them customer access; validate separately before disclosure. Do not request passwords, MFA codes, keys, raw connection strings or unrestricted customer exports.

3. Priorities and conflicting targets

The reviewed sources contain three different schemes. Do not silently merge them into a new customer commitment.

Source position	Exact target position	Status / action
Website Support page [S4]	Critical: 4 business hours. High: 1 business day. Normal: 2 business days.	Published in the reviewed website repository. Listed as indicative initial-response targets; calendar not defined there.
Earlier service-level draft [S1]	P1: 1 hour. P2: 4 business hours. P3: 1 business day. P4: 2 business days.	Proposed, not an executed SLA. P1 does not explicitly say business/elapsed hour; resolve before use.
Engineering incident runbook [S7]	SEV-1: immediate. SEV-2: triage within 30 minutes. SEV-3: during the support day.	Engineering handling expectations, not customer-response or staffed-coverage evidence.

Proposed case classification (retain P1-P4)

Priority	Triage basis
P1 - Critical	Production unavailable, widespread authentication failure or credible serious security/data-integrity concern. A single-customer serious exposure can be P1; customer count alone is not decisive.
P2 - High	Major function or critical integration materially impaired with significant business impact and no reasonable workaround.
P3 - Medium	Feature impaired but productive use remains possible, usually with a workaround.
P4 - Low	How-to, minor defect or routine non-urgent configuration request. New product work is recorded separately as an enhancement.

Assess impact and urgency using customer evidence. Security keywords trigger immediate review, not blind severity assignment. A credible security concern follows the existing precautionary P1 path until understood; an authorised lead records any downgrade and reason. [S2-S3]

Decision D01 - recommended launch approach

Keep the current published indicative target set as the proposed launch baseline; provisionally map P1 to Critical, P2 to High and P3/P4 to Normal. This mapping is a recommendation, not approval. Faster draft/engineering targets may be internal stretch goals only where staffed and agreed. Resolve the final scheme in T1 before changing public material.

4. Service clock and escalation

A receipt acknowledgement, meaningful response, restoration and permanent resolution are different events.

Calendar decision before activation

The earlier draft proposes 08:00-18:00 Australian Eastern Time, Monday-Friday, excluding Australian national and ACT public holidays. No staffed roster is established by that proposal. The support schedule must select the time-zone identifier, applicable holiday calendar and daylight-saving treatment for AU, NZ and Singapore customers. [S1]

Proposed clarification: use Australia/Sydney for that eastern calendar, accrue only covered minutes, and define one business day as 10 covered hours if the 08:00-18:00 window is approved. This is a new interpretation for approval, not the meaning silently assigned to existing agreements. A customer agreement may specify something different.

Event / clock	Proposed rule to implement after approval
Receipt	Capture the first accepted receipt on the agreed channel, even if ticket creation is delayed. Store UTC plus the applicable customer/service calendar.
Initial response	A person acknowledges the actual issue, confirms ownership/triage and states the next step. An automatic email alone does not satisfy this metric.
Outside coverage	For business-time targets, accrual begins at the next covered period. An out-of-hours email is not a promise of out-of-hours monitoring. Only a separately staffed/contracted emergency route changes that.
Waiting / transfer	Do not pause or reset initial response for internal queues, suppliers or missing customer detail. Give a meaningful response first. Later clocks pause only if the contract allows, with reason and timestamps.
Restore / resolve	Restore means useful service or an accepted workaround is available. Resolve means the agreed case outcome is delivered. Track gross elapsed outage as well as any contractual exclusions.
Priority change	Retain original receipt, all priority history and old deadlines. Recalculate against the agreed rule; do not restart the case clock to hide lateness.

Escalation that cannot disappear into a queue

On P1 assessment, assign an incident lead and contact L3/security as applicable. Escalate immediately to the backup when the owner is unavailable or the next update/response is at risk; do not wait until the target expires. L2/L3 must explicitly accept a technical handoff. Support retains the customer case and update schedule throughout.

Illustration only

With an approved 08:00-18:00 calendar and a four-covered-hour target, a 17:00 receipt is due at 11:00 on the next covered day. A weekend/holiday is skipped. No live target is established by this example.

5. Case management procedure

One customer-facing record, one accountable owner, and a linked technical record where needed.

1. Receive and acknowledge. Create a unique ID or use the controlled fallback. Preserve receipt time and show the applicable coverage statement.
2. Verify and triage. Confirm organisation/environment and disclosure authority, classify the request, assess impact and capture a safe evidence set.
3. Investigate or hand off. Check known issues, release history, health and source status. Resolve using an approved procedure or obtain explicit L2/L3 acceptance.
4. Communicate and verify. State the next action and next update time, including when there is no material change. Validate restoration with the appropriate customer user.
5. Resolve, close and learn. Record the outcome and closure basis, preserve linked defects/problems, and identify reusable knowledge.

Status (retain existing terms)	Required condition / ownership
New / Triage	Received / under assessment; named queue owner must prevent unattended cases.
In Progress	Named case owner is coordinating work, including customer/supplier dependencies.
Waiting for Customer	A specific information/action request and reminder time are recorded. Clock treatment follows T1, not a blanket pause.
Waiting for Engineering	Linked technical item has an accepting resolver; support keeps updates and customer ownership.
Resolved / Closed	Outcome sent / accepted or approved closure policy completed. Retain a reopening route and original history.

Minimum record and automation controls

Retain case ID, organisation, requester, environment, type, product/integration, impact, priority, owner, status, receipt/response/deadline timestamps and linked technical item. Add contract-calendar reference, next update, safe evidence link, disclosure scope and escalation acceptance. Use T3.

Email-channel forms must remain email-compatible; collect additional fields during triage. Test acknowledgement, threading, duplicate handling, attachment restrictions and internal-note separation. Do not auto-share a case to everyone with the same email domain. Security cases require restricted visibility. [S2]

Proposed closure default for ordinary cases: notify resolution, seek confirmation, remind, then administratively close after three covered business days without further reply. Approve the period first. Do not auto-close unresolved P1/security cases. Reclassification as an enhancement must not disguise an unresolved incident or imply product delivery.

6. Major incident and security path

Protect the service and evidence. Communicate verified facts. Avoid unapproved production intervention.

1. Declare and assign. Record incident/case IDs, UTC detection time, affected scope, known impact and a named incident lead. Separate confirmed facts, suspicions and unknowns.
2. Establish the baseline. Capture correlation IDs, deployed release, recent changes and applicable health/monitoring evidence. Determine whether the fault is local, tenant-specific or broader.
3. Contain safely. The authorised technical/security lead selects a reversible containment action with recorded authority. Preserve evidence before destructive steps where possible; do not delay urgent authorised containment just to collect perfect evidence.
4. Coordinate and communicate. Link affected cases to a restricted incident record. Assign technical workstreams and a customer communications owner. Agree and record the next update time even when there is no ETA.
5. Restore and validate. Use the approved recovery/change procedure, validate dependencies and a customer workflow, then monitor stability. A health endpoint alone is insufficient.
6. Review and close. Record impact, timeline, actual restoration time, data-loss assessment, remaining fixes and evidence. Track corrective actions with owners and dates.

Security-specific decisions

Follow the existing precautionary P1 escalation for suspected unauthorised access, exposure, compromise or material control failure until assessed. Restrict logs and evidence to authorised responders. Use controlled test tenants for reproduction; never probe another customer's production data. Avoid public speculation about scope or attribution. [S3, S7]

The security lead and accountable service owner must promptly assess applicable customer-contract, privacy and regulatory notification requirements with appropriate advice. Record jurisdiction, awareness time, potential deadline and approver. No universal notification deadline is assumed in this pack, and notification assessment must not wait for a complete root cause.

Communication cadence - proposed planning defaults

During actively staffed response, propose P1 updates every 60 minutes and P2 updates every four covered hours, adjusted to impact and the agreed service schedule. Send material changes sooner. Publish the actual next-update timestamp and zone. These proposed defaults do not create continuous coverage.

Do not claim

Do not say "no data was affected" without evidence; use "the assessment remains in progress". Do not promise a restoration time merely to fill an update. Do not run historic hard-coded environment commands without target verification and authority.

7. AIDE Ops and operational visibility

The service desk owns cases. AIDE Ops provides cross-system oversight, with data quality visible.

Signal / authoritative evidence	Operational response and owner
Unowned or overdue case / service desk	Support lead assigns owner/backup and confirms a next action. AIDE Ops may surface the signal only after its case-source mapping is accepted.
Service liveness/readiness / deployed platform monitoring	Technical lead distinguishes process failure from dependency failure, validates customer impact and opens/links an incident.
Heartbeat / AIDE publisher	A heartbeat indicates that a publisher communicated. It does not refresh a separate usage record or prove every workflow is healthy.
Usage / accepted, mapped observation	Review timestamp, organisation mapping and provenance. Zero recorded activity is not automatically churn or an outage.
Integration health / current source evidence	Do not infer health from an old successful import. Missing connector-health evidence remains unknown/partial, not zero failures.
Queue delivery / collector, inbox and worker	Where implemented, verify accepted, processed and reconciled events separately. An HTTP acknowledgement is not proof the worker updated the control room.
Customer health / multiple agreed sources	Keep account mapping, known data gaps and review ownership explicit. Do not present an incomplete score as a fully observed customer condition.

Known repository semantics, not deployment certification

The reviewed operations/usage reference documents separate heartbeat and signed usage updates, organisation allowlisting and aggregate-only export. It distinguishes purchased seats, activated accounts, logins and meaningful product activity. It explicitly omits facts such as reliable integration-health and renewal dates where sources do not establish them. [S6]

This review has not executed a live Ops acceptance test or verified the current connector configuration, worker processing, email delivery or ITSM handoff. Verify each required source against the deployed versions before declaring the operations layer ready.

Minimum monitoring acceptance

Record signal owner, detection rule, observation timestamp, freshness threshold, routing destination, sample event, expected response and last successful end-to-end test. Send synthetic faults to a safe test route. Suppression must be authorised, time-bounded and visible; restore the rule after testing.

Fallback while integration is incomplete

A named person can inspect the authoritative service desk and platform monitoring during agreed coverage using a recorded checklist. Do not describe an unconfigured connector as automation that is already protecting the service.

8. First-line troubleshooting cards

Collect evidence and use approved actions. Escalate before exceeding access or change authority.

Symptom	Safe initial checks and escalation
Cannot sign in / MFA / password recovery	Confirm customer and known contact; scope affected users and error/time. Check for a wider authentication issue and account/entitlement state. Do not request codes or bypass MFA. Escalate suspicious access or privileged recovery.
Missing projects / unexpected access	Confirm selected organisation and authorised project grants without revealing other tenants. Treat a credible isolation failure as critical; preserve correlation/audit evidence and engage security/L3.
Incorrect subscription or seat access	Compare approved order and product entitlement through authorised views. A configured seat count is not proof of payment. Escalate billing reconciliation; do not charge/refund or grant seats to fix a symptom without approval.
Connector stopped refreshing	Check approved source, last successful observation, mapping, permissions, rate-limit/error evidence and recent credential changes. Do not repeatedly retry destructive or non-idempotent operations. Coordinate with the source owner.
Stale evidence / misleading control signal	Check observation time, reporting period, mappings and baseline. Preserve the actual unknown/stale status; do not edit evidence or tolerances just to produce green.
Blueprint gaps or unexpected discovery result	Confirm the scoped domain, source provenance, reconciliation decisions and model version. Preserve architect approval rights; discovery observations are not automatically an approved target state.
Report/export missing or failing	Capture job/time/correlation ID; check scope and permissions, underlying evidence and artifact storage. Do not make storage public or send another tenant's artifact.
Service down / repeated application errors	Check the correct environment's liveness/readiness and deployment version; inspect approved telemetry. Open/escalate the incident. Restarts and release rollback belong to the authorised technical change path.
Ops card stale / event accepted but absent	Distinguish heartbeat, usage and mapping timestamps; inspect the correct receiver/worker/source through approved access. Preserve unknown/partial status until reconciliation is evidenced.

Engineering handoff must be usable

Provide customer/environment, severity and impact, first/last observed times, safe reproduction steps, current version, correlation/evidence references, changes checked, attempted actions and their results, workaround, disclosure restrictions and next customer update. Record the accepting resolver and acceptance time in T3.

9. Change, recovery and continuity

Use controlled technical runbooks; do not copy stale commands into customer-facing material.

Release or configuration change

Record the exact target, release/configuration version, reason, impact, authoriser, test evidence, rollback path and post-change checks. For an emergency, preserve the decision trail and retrospective review. A previous runbook's example resource group, application name or direct-to-main instruction is not authority to change the current customer environment.

Where a rollback includes database/schema changes, prove compatibility first. Reverting code alone may not revert data safely. Maintain separation between runtime and privileged recovery work; do not patch production files ad hoc. [S7-S8]

Recovery objectives require environment-specific evidence

Service / store	Record before approving a recovery commitment
Product database and artifacts	Agreed data-loss/recovery objectives, protection settings, retained recovery points and measured drill results.
Support case store and AIDE Ops	Separate state/export protection, recovery owner and validation evidence; product recovery does not prove support recovery.

Planning values in a technical runbook are not proof of current configuration, a contractual promise or end-to-end recovery. Validate the actual environment and record measured drill outcomes. Do not infer recovery commitments for case records or AIDE Ops from product evidence.

1. Authorise and scope. Declare the incident/change, select the recovery point and document the expected data gap, owners and customer impact.
2. Restore separately. For PostgreSQL, restore to a new target; validate schema, tenant scope and evidence before changing production connectivity. Restore only the intended Blob version/object via controlled access.
3. Validate service. Test login, tenant boundaries, an agreed Chain or Blueprint workflow and relevant reports/artifacts. Reconcile data/metadata consistency, monitor new requests and obtain customer/service-owner acceptance.
4. Retain and clean up safely. Keep the original recovery source until acceptance. Delete only verified temporary test resources after evidence capture and authority; never treat a copied cleanup command as safe for production.

Support and Ops continuity
Give the case store, approved contact roster, Ops configuration/state and restricted evidence their own backup/export, access and recovery ownership. A product database drill alone does not prove the support service can survive an outage.

10. Readiness and service rehearsal

Do not activate a service promise before someone other than the author can execute it.

Gate / safe rehearsal	Acceptance evidence
Ownership and coverage	Named service owner, primary, backup and technical/security escalation have accepted coverage and handover.
Approved schedule	One selected target set, calendar, clock rules, scope and exclusions are approved in T1; public/draft inconsistencies resolved.
External intake round trip	Test email/request, unique case, acknowledgement, meaningful response, same-case customer reply, attachment and resolution.
Access separation	Test two synthetic organisations. One cannot view the other's cases or internal notes. Validate requester/privileged-change verification.
Outside-hours clock	Simulate near-close, weekend/holiday, priority change and waiting statuses. Compare expected versus actual deadlines; no misleading reset or pause.
Escalation and absence	Simulate owner unavailable, P1 and at-risk deadline. Backup/resolver receives and accepts responsibility; customer updates remain owned.
Monitoring and Ops	Inject or replay approved synthetic events. Verify detection, delivery, processing, mapping and visible stale/unknown states; no real customer incident triggered.
Intake / application outage	Use the independent fallback while sign-in or ticketing is unavailable; reconcile the manual case and original receipt time afterwards.
Recovery evidence	Technical owner identifies the current approved runbooks and last drill. Any missing mandatory recovery evidence is recorded as a hold.
Handover and go-live	Receiving service owner accepts the roster, known issues, runbooks and customer schedule; approvers record go/hold and evidence references.

Test safely

Use synthetic identities, segregated test organisations and clearly labelled notifications. Agree the window and recipients. Do not interrupt live customers, disable production controls, charge subscriptions or restore databases merely to complete a desktop rehearsal.

T7 is an unexecuted test record, not a completed assurance report. Use Pass / Fail / Not run / N/A with reasons and evidence. A mandatory failed or untested gate is a hold; an exemption needs explicit authority and must not contradict contract or legal requirements.

Activation outcome

Pass means the minimum agreed service can operate with evidence. It does not certify the product or justify broader availability, security, on-call or recovery claims.

11. Operating rhythm and handover

Use a small number of signals that lead to action, not a dashboard that merely looks healthy.

Cadence - proposed	Activity and evidence
Start/end of covered shift	Review new/unowned cases, priority incidents, due responses/updates, integration/monitoring gaps and named backup. Record the receiving person for unfinished work.
Weekly service review	Review volume, breaches, repeated incidents, customer friction and available support capacity. Assign the few highest-value corrective actions.
Monthly control review	Check contact/role changes, supplier access, support-channel tests, known issues, runbook currency and recovery evidence; reconcile operational commitments with contracts.
After a major incident	Proposed review within five covered business days of stabilisation, adjusted by the incident lead. Separate prompt notification/action from the later root-cause review.
Per customer handover / renewal	Confirm service scope, schedule, authoritative sources, open risks, contacts, retention/exit and review dates. Expansion does not silently expand support coverage.

Measures and definitions

Measure	Definition and owner
First response compliance	Meaningfully responded cases within their applicable target / eligible cases due in the period. Include overdue unanswered cases as failures; identify not-yet-due exclusions. Support lead.
Unowned / update overdue	Count and age of cases without an accepting owner or with next_update_due passed. Include internal/supplier-waiting work. Support lead.
Restore / resolve time	Report detection/receipt-to-restoration and receipt-to-resolution separately, including gross elapsed time and any agreed clock exclusions. Incident lead.
Recurrence / reopened cases	Track repeat causes and reopened resolutions with linked problem records; do not count every duplicate alert as a distinct incident. Product lead.
Demand / capacity	Cases and effort by customer, type and severity; compare with actual staffed capacity and coverage. Service owner.
Evidence freshness	For each required source, measure last accepted observation, stale/unknown duration and last routing test. A healthy heartbeat cannot satisfy another source's freshness. Technical lead.

A service handover is complete when T6 is accepted, not just when the customer environment exists. Preserve the onboarding guide's hypercare approach: agreed duration, no unresolved critical incident, accepted major-issue plans, independent administration, stable priority integrations and a successfully exercised support route. [S5]

12. Decisions before launch

Each item remains open until an authorised person records the decision and evidence.

ID / decision	Proposed position or required evidence	Accountable role
D01 - Response targets	Select website baseline or approve another set; resolve P1 one-hour ambiguity and distinguish engineering severity. T1 contains the final schedule.	Service owner
D02 - Calendar / clocks	Approve hours, zone, holidays, business-day meaning, after-hours route, pause rules, update cadence and closure period.	Service owner
D03 - Staffing / partner	Name accepting L1, backup, L2/L3/security contacts. Any provider requires an actual agreement and tested access.	Service owner + provider
D04 - Case platform / intake	Confirm Jira Service Management or agreed partner ITSM; test mailbox/portal and independent fallback. Do not publish an untested address as monitored.	Support lead
D05 - Ops acceptance	Verify deployed version compatibility, signal ownership, customer mapping, worker/routing tests and visible data gaps. Preserve unknown state.	Technical lead
D06 - Recovery / privacy	Revalidate product and support/Ops recovery evidence, service objectives, access, evidence retention and customer-specific notification escalation.	Technical/security lead
D07 - Contract / publication	Approve customer service schedules, reconcile website claims and keep reference material separate from contractual commitments. Completed records and detailed technical runbooks remain controlled.	Authorised commercial owner
D08 - Rehearsal / activation	Complete T7 with a second operator; rectify mandatory failures; record go/hold, review date and known limitations.	Service owner + reviewer

A practical implementation order

1. Decide. Complete D01-D04 and nominate the people. This is the minimum structure required to configure correctly.
2. Configure and exercise. Set up the approved case workflow, clocks, access and routing; validate D05-D06; perform T7 with synthetic data.
3. Approve and communicate. Complete D07-D08, issue the accepted customer schedule and handover, and issue only approved operational service commitments. Rehearse again after material changes.

What this work has and has not done

This task creates the pack and templates. It does not send support announcements, configure Jira/Microsoft 365/AIDE Ops, bind a partner, approve service levels or run the live rehearsal. Publishing this reference draft does not change existing website support promises.

13. Sources and document control

Source-derived positions are retained; new detailed operating rules are clearly proposed.

Ref.	Source reviewed and use
S1	Prior Customer Support and Service Levels working draft: proposed channel, 08:00-18:00 AET coverage, P1-P4 targets, scope and customer responsibilities.
S2	Prior Support Case Management Procedure working draft: proposed JSM/email setup, case fields, queues, automation, access/privacy and implementation tests.
S3	Prior Internal Support Operations Runbook working draft: L1/L2/L3, triage/statuses, P1/security handling, problem management and measures.
S4	Website Support page (support.html), reviewed 5 October 2026: indicative Critical 4 business hours, High 1 business day and Normal 2 business days. No staffed-coverage verification is implied.
S5	Public Sales, Pilot & Onboarding Guide v1.0, 5 October 2026, and companion templates. Sections 6-8 require tested support, readiness acceptance and handover.
S6	Controlled product operations/usage reference: heartbeat/usage separation, allowlisting, data meanings and missing health evidence. Not live acceptance evidence.
S7	Controlled engineering incident/recovery reference: severity, diagnosis, evidence protection and recovery checks. Historic example targets are not executable instructions.
S8	Controlled backup/recovery reference: planning objectives, separate-target restoration and drill evidence; not current configuration proof.

Control and distribution

Prepared 5 October 2026; version 0.1; maintainer: JEL Project Management; status: public reference draft, not an activated service schedule. Review after operational activation, a material incident, service change or new contractual requirement. No earlier agreement is superseded by this draft.

This public edition removes unconfirmed provider references, personal assignments and private repository identifiers. The source working drafts remain controlled. Completed forms, customer contacts, environment details, incidents and evidence must never be uploaded to the public website. Publication is not service activation.