SOTERIA CLOUD SUPPORT

Support Operations Manual

A practical internal guide for classifying, triaging, communicating, escalating, resolving, documenting, and improving Soteria Cloud support requests.

Internal use | 9x5 support | 24x7 valid DR incidents | Acronis escalation

Operational Standard

Provide calm, predictable, outcome-driven support that protects customer recoverability, partner confidence, and service stability.

Acronis **Acronis-powered services**

Soteria Cloud delivered

START HERE

Every ticket must have clear ownership, priority, next action, and evidence.

Support agents should first identify who is asking, what is impacted, how urgent the request is, what coverage applies, and which ownership path must be followed.

Requester type

Direct customer, reseller/MSP/partner, affiliate, or internal Soteria team.

Request type

Incident, service request, restore, disaster recovery, enablement, vendor issue, billing, licensing, or security concern.

Priority

P1 through P4 based on business impact, urgency, affected users, and whether recovery is required.

Coverage

Business-hours support for normal requests; 24x7 only for valid disaster recovery incidents.

Authorization

Confirm authority before restore, deletion, overwrite, failover, failback, or configuration changes.

Documentation

Record actions, approvals, timestamps, evidence, vendor case numbers, updates, and closure outcome.

PRIORITY MATRIX

Classify by business impact and recovery urgency.

P1 is reserved for production outage, active cyber incident, major data loss, failed urgent recovery, or a valid disaster recovery incident.

PRIORITY	COVERAGE	INITIAL RESPONSE	UPDATE RHYTHM	RESOLUTION APPROACH
P1 Critical / DR	24x7 for valid DR incidents	30 minutes	Every 60 minutes during active incident	Best effort until service restored or recovery path agreed
P2 High	9x5 business hours	2 business hours	Daily or as agreed	Best effort based on complexity
P3 Normal	9x5 business hours	1 business day	Every 2 business days or as needed	Best effort based on queue and complexity
P4 Low / Enablement	9x5 business hours	2 business days	As needed	Best effort

P1 DR TEST

Treat as P1 only when production operations are materially impacted and urgent recovery, failover, or cyber recovery action is required.

NOT P1

Routine restores, test restores, backup policy changes, licensing questions, reports, training, and general how-to requests stay in standard 9x5 support.

OWNERSHIP

Know who owns the customer communication before acting.

The same technical request is handled differently depending on whether Soteria Cloud, a partner, or an affiliate owns the customer support relationship.

Direct customer

Soteria Cloud owns first-line support, investigation, Acronis interaction, restore guidance, DR coordination, communication, closure, and follow-up.

Partner customer

The partner owns first-line support, context gathering, authorization, and customer communication unless a separate managed support agreement exists.

Affiliate customer

Soteria Cloud owns support end to end unless a separate written agreement states otherwise.

PARTNER BOUNDARY

Soteria Cloud supports the partner with enablement, platform guidance, escalation support, vendor escalation, DR assistance, and best-practice recommendations.

END CUSTOMER CONTACT

If a partner-managed end customer contacts Soteria directly, avoid unauthorized changes and route through the partner unless valid DR risk requires urgent action and authority is confirmed.

TICKET MOTION

Use repeatable paths for the most common request types.

Agents should keep each workflow moving with clear status, business-impact context, and documented next actions.

Standard Ticket

Standard Ticket workflow

1. Receive the request through an approved support channel.
2. Identify requester type: direct customer, reseller/MSP/partner, affiliate, or internal team.
3. Confirm scope, authorization, supported customer path, and support coverage.
4. Classify request type and priority using the matrix.
5. Triage tenant, workload, user, service, policy, backup, restore point, or error evidence.
6. Resolve directly, escalate internally, or escalate to Acronis with evidence.
7. Communicate current status, next action, required input, and next update timing.
8. Confirm outcome, record the support story, capture lessons, and close.

P1 DR Incident

P1 DR Incident workflow

1. Acknowledge within the target SLA and open a P1 incident record.
2. Confirm requester authority, business impact, affected systems, and production impact.
3. Identify last known good backup, restore point, or available recovery option.
4. Confirm recovery objective: restore, alternate restore, failover, export, or selected recovery.
5. Get explicit approval before destructive, overwrite, failover, or irreversible actions.
6. Start recovery actions and update every 60 minutes while active.
7. Escalate to Acronis if a platform defect or recovery blocker is suspected.
8. Continue until service is restored, workaround is active, or recovery path is formally agreed.
9. Document timeline, approvals, evidence, vendor cases, and post-incident actions.

RECOVERY SUPPORT

Restore and backup issues must be handled with approval, evidence, and validation.

Do not take destructive action or overwrite production data without confirmed authority and written approval where required.

Restore Request

Restore Request workflow

1. Confirm requester authority and supported customer relationship.
2. Confirm customer, tenant, affected workload, data type, and restore destination.
3. Confirm restore point, date, time, overwrite risk, and business impact.
4. Get written approval for overwrite, deletion, failover, failback, or data-loss risk.
5. Execute or guide the restore using the approved path.
6. Validate restored data or service usability with the requester.
7. Close with restored item, restore point, destination, result, and any follow-up action.

Backup Failure

Backup Failure workflow

1. Confirm affected customer, device, policy, and whether the workload is critical.
2. Check last successful backup and current error evidence.
3. Identify whether the cause is local, agent, credential, storage, network, policy, application-aware, operating system, or platform-related.
4. Apply a known fix, request required customer or partner action, or escalate.
5. Run or request retry and confirm success.
6. Escalate repeated failures or multi-customer patterns to operations leadership.

ESCALATION

Partner enablement and Acronis escalation need different evidence and expectations.

Enablement builds partner capability. Vendor escalation requires validated evidence, clear business impact, and active communication of dependencies.

Partner Enablement

Partner Enablement workflow

1. Confirm partner, customer context, and use case.
2. Decide whether the request is enablement, support, or an active incident.
3. Provide concise steps, best practice, or documentation.
4. Explain enough for the partner to become more capable.
5. Route deeper training or implementation review through the partner enablement path.
6. Close with next action and any reusable documentation improvement.

Acronis Vendor Escalation

Acronis Vendor Escalation workflow

1. Validate the issue locally and rule out obvious configuration, local, or operational causes.
2. Confirm business impact, urgency, and priority.
3. Gather tenant, datacenter, workload, error, logs, timestamps, screenshots, reproduction steps, and actions already tried.
4. Open the Acronis support case and record the case reference in the Soteria ticket.
5. Communicate vendor dependency clearly to the customer or partner.
6. Follow up with Acronis and keep the requester updated until workaround or resolution.

COMMUNICATION STANDARD

Updates must be clear, calm, business-impact focused, and specific about next steps.

Good support communication reduces pressure because the requester knows what is happening, what is needed, and when the next update will arrive.

Good update format

Current status. What we found. What we are doing next. What we need from you. Next update by.

Avoid

Technical fog, overpromising, blame language, unsupported vendor claims, emergency misuse, or destructive actions without approval.

P1 OPENING SUMMARY

Customer, affected workload, impact, requested recovery outcome, current action, owner, and next update time must be visible early.

CLOSURE SUMMARY

Include what happened, what was done, result, requester validation, remaining risk, vendor reference, and any follow-up action.

OPERATIONAL HYGIENE

Every ticket should improve visibility, confidence, or the support model.

Use the intake checklist and monthly metrics to make support measurable and easier to improve.

Ticket intake

Requester, company, contact, tenant, affected asset, request type, business impact, urgency, evidence, backup status, restore point, approval, and priority.

Monthly review

Tickets by priority and requester type, SLA response, P1/P2 incidents, restore requests, failed backups, vendor escalations, enablement, repeat issues, and root causes.

Boundaries

Support excludes unrelated general IT support, unauthorized changes, customer hardware replacement, unsupported custom integrations, and partner first-line replacement unless contracted.

IF UNSURE

Ask. Escalate early when impact is high.

IF IT MATTERS

Document it in the ticket.

BEFORE CLOSURE

Verify satisfaction or confirm the next path.