# Escalate with the context needed to act.

Prepare a clear support escalation when an issue exceeds the current responder’s authority or capability.

## Escalation handoff

| Include | Why it helps |
|---|---|
| Impact | Explains the urgency and affected workflow |
| Timeline | Shows what changed and what has been tried |
| Evidence | Links relevant traces without exposing secrets |
| Decision needed | Identifies the authority or expertise being requested |

## Preserve ownership during the handoff

An escalation is not complete when a message is sent. Confirm who owns the next action and when the reporting team should expect an update.

## Avoid repeating unsafe recovery attempts

Document actions already taken and their results. The next responder should not unknowingly repeat a destructive or ineffective step.

## Choose the appropriate support route

For a system covered by an existing agreement, use the reporting and escalation channels established in that agreement. They define the information required, service availability and response arrangements. A general website resource cannot change those commitments or establish an emergency channel.

For an initial discussion, describe the application and the task that needs attention. State whether this is a defect, a maintenance question, a proposed improvement or an active incident. Distinguishing these situations helps avoid sending a business-critical failure through a new-project conversation. The support form lets you send the details by email or download a local PDF copy. Emailing the request does not create a ticket in an external service desk or establish a response time.

## Prepare a report that can be investigated

Include the affected environment, approximate time, observed behaviour and expected result. Describe the scope of the impact, such as a particular user role or set of records. Add relevant request identifiers and steps that reproduce the issue, using redacted examples where possible. Record recent changes without assuming they caused the problem.

Do not include passwords, access tokens or unrestricted copies of customer documents. If sensitive evidence is needed, agree an appropriate transfer method through the established support channel. Explain any actions already taken, including retries, configuration changes or restarts. This prevents responders from repeating work or overlooking a state change introduced during initial investigation.

## Keep investigation and improvement connected

During investigation, maintain a shared account of the current impact, actions taken and next decision. Distinguish a temporary workaround from a verified correction. If records may be inconsistent, assign responsibility for identifying and reconciling them rather than assuming a code fix repairs historical data.

After the issue is resolved, record the cause where it is known and the evidence supporting the conclusion. Identify useful follow-up work in tests, monitoring, documentation or interface design. A recurring problem should become a prioritised improvement rather than a permanent support ritual. Review the support boundary when the system changes so new dependencies and responsibilities are covered deliberately.

## Does submitting the support form trigger an escalation?

No. The current website prepares a local report only. Use the contact path and coverage established in your support agreement.

## Read the current resource online

https://cobnex-review.rgcsekaraa.workers.dev/trust-hub/abuse-approach/