

# P0 Incident Response Procedure

INTERNAL — Helix Engineering / CS Operations

## PURPOSE

Define the response protocol for P0 incidents — incidents that materially impact paying customers' ability to use Helix's core functionality.

## DEFINITION OF P0

A P0 incident is any of the following: (1) more than 5% of customers cannot log in, (2) workflow runs are failing at >10% rate workspace-wide, (3) data loss has occurred or is occurring, (4) a security breach has been detected, or (5) the API is returning 5xx errors at >5% rate.

## INITIAL RESPONSE

Within 5 minutes of detection: (1) Page the on-call engineer via PagerDuty. (2) The on-call declares the incident in #incidents Slack and creates an Incident Commander (IC) role. (3) IC opens a Zoom bridge and posts the link in #incidents.

## COMMUNICATION

The IC is responsible for status page updates. Post initial status within 10 minutes of declaration. Update the status page at <https://status.helix.io> every 15 minutes minimum until resolution.

## ESCALATION

If the on-call engineer cannot identify root cause within 30 minutes, escalate to the secondary on-call. If both on-calls are unable to make progress within 60 minutes total, page the engineering manager.

## EXTERNAL COMMUNICATION

For any P0 lasting longer than 30 minutes, send an email update to all paying customers. Use the pre-approved template in /docs/incident-templates. CS leadership must approve before sending.

## RESOLUTION

When the incident is resolved: (1) Mark the status page resolved. (2) Send a final email update if customers were notified. (3) Schedule a postmortem within 5 business days.

## POSTMORTEM

Postmortem is required for all P0 incidents. Use the postmortem template. Blameless culture: focus on systems, not individuals.