PROJECT 042 - WORKFLOW NOTES

AI Agent + Tools + Human Approval System | n8n • PostgreSQL • Slack • Human-in-the-Loop

Technical reference: Documents node responsibilities, data flow, approval logic, validation, testing, and safeguards for the completed two-workflow system.

WORKFLOW 01 - MAIN AI OPERATIONS AGENT

Objective: Conversational operations interface that can retrieve business data autonomously while converting protected order-status changes into Pending human-approval requests.

1. Receive Operations Request

Chat trigger receiving the user's natural-language request and active session context.

2. AI Operations Agent

Central orchestrator. Interprets intent, selects tools, coordinates reasoning, and generates the response.

3. AI Reasoning Model

LLM used for language understanding, reasoning, tool selection, and response generation.

4. Conversation Memory

Maintains short session context so follow-up requests can reference earlier messages.

5. Order Lookup

PostgreSQL read tool for order records and current order status; also used before a requested status change.

6. Customer Lookup

PostgreSQL read tool for customer details and customer-level context.

7. Operations Intelligence

PostgreSQL read tool for broader operational questions and structured business-data retrieval.

8. Request Human Approval

Protected-write tool that creates a unique Pending approval instead of directly modifying the order.

Workflow 01 Logic & Guardrails

- Read request: Agent may use lookup/intelligence tools and return the result.
- Write request: Agent checks the target record, then creates a Pending approval request.
- Critical guardrail: Creating the approval must not modify the target order.
- Response: Return order ID, current status, requested status, approval ID and Pending state, explicitly confirming no update has occurred.

Handoff Data to Workflow 02

Field	Purpose
approval_id	Unique link between AI request, human decision, execution, and audit record.
order_id	Target order that may be changed only after authorization.
requested_status	Proposed new order status awaiting human approval.

Workflow 01 Test Evidence

Validated with order lookups and protected-write requests. Example: ORD-1051 was read as Processing; a request for Ready for Dispatch generated a unique Pending approval while the agent explicitly confirmed that the order had not yet been modified.

WORKFLOW 02 - HUMAN APPROVAL & ORDER UPDATE

Objective: Validate a pending request, obtain a human Slack decision, re-validate before execution, route Approve/Reject, communicate the result, and persist an audit record.

A. APPROVAL REQUEST & NOTIFICATION

Receive Approval Request
Webhook receives approval ID, order ID, and requested status.

Lookup Pending Approval
Queries PostgreSQL for the authoritative stored approval record.

Validate Approval Status
Allows the request to proceed only when a valid Pending approval exists.

Send Slack Approval Card
Posts approval ID, order ID, requested status/action, and interactive Approve/Reject controls.

B. HUMAN DECISION & VALIDATION

Receive Human Decision
Webhook receives the Slack interaction payload.

Parse Approval Decision
Normalizes the Slack payload into decision and approval-reference fields.

Retrieve Approval Request
Reloads the authoritative approval record after the human decision.

Validate Still Pending
Second state check immediately before execution; blocks stale or already-resolved approvals.

Route Approval Decision
Deterministically routes the verified human choice to Approved or Rejected execution.

C. CONTROLLED EXECUTION & AUDIT

APPROVED PATH	REJECTED PATH
Approve & Update Order - performs the authorized status update. Send Approval Confirmation - posts success to Slack. Log Approved Action - records the approved execution in PostgreSQL.	Reject Request - resolves the request without applying the proposed order change. Send Rejection Confirmation - posts the rejected result to Slack. Log Rejected Action - records the rejection for traceability.

Testing Checklist

- Lookup: Ask for an order/customer detail and confirm only the necessary read tool executes.
- Approval creation: Request a status change; verify a fresh Pending approval exists and the order remains unchanged.
- Slack card: Verify approval ID, order ID, requested status/action, and Approve/Reject buttons.
- Approve: Use a fresh request; verify update → Slack confirmation → Approved audit log.
- Reject: Use another fresh request; verify no order update → rejection confirmation → Rejected audit log.
- Do not reuse processed approval IDs: Each full approval/rejection test should begin with a fresh Pending request.

Audit Log

The activity log preserves request_id, user_request, intent, tool_used, target_id, approval_required, approval_status, execution_result, agent_response, and created_at so the action can be reconstructed later.

Maintenance & Safety Notes

- Use parameterized PostgreSQL queries and keep SQL placeholders aligned with supplied parameters.
- Do not connect arbitrary test branches directly to database-write nodes for screenshots; manual execution can alter PostgreSQL data.
- Use fresh simulation records and verify database state before and after write tests.
- Keep read tools separate from protected writes; the agent requests authorization rather than bypassing Workflow 02.
- Preserve the second Pending validation before routing/execution as a stale-request and duplicate-action safeguard.
- For production: add webhook authentication/signature verification, least-privilege DB credentials, error/retry handling, and dev/staging/production separation.

Completed Outcome

Two coordinated workflows now provide agentic data retrieval plus deterministic human authorization for consequential changes. Both Approved and Rejected paths were tested, Slack outcomes were confirmed, and PostgreSQL audit records were produced.