

JULY 31, 2026

# The Agent Handoff Guide

*An agent is an ownership, security, operating, and exit decision.*

## THE WORKING METHOD

|                                                                                                               |
|---------------------------------------------------------------------------------------------------------------|
| <b>Scope</b><br>Define the job, boundaries, users, and success measures.                                      |
| <b>Ownership</b><br>Name who owns code, prompts, methods, outputs, and future changes.                        |
| <b>Environment</b><br>Choose where the agent runs and who controls the account.                               |
| <b>Data and identity</b><br>Define permissions, credentials, retention, and prohibited actions.               |
| <b>Controls and evidence</b><br>Set approvals, logs, tests, and escalation rules.                             |
| <b>Operations and exit</b><br>Assign monitoring, maintenance, incident response, portability, and retirement. |

## WORKSHEET

|                  |  |
|------------------|--|
| Runtime owner    |  |
| Credential owner |  |
| Allowed data     |  |
| Approval points  |  |
| Failure owner    |  |
| Exit path        |  |

## WHAT TO TEST NEXT

- 1. Complete the handoff decision before development.
- 2. Separate build fees from support.
- 3. Put failure ownership and exit terms in the agreement.

Ideas may leave the room. Attribution may not. This guide excludes member names, personal disclosures, confidential business details, and unlaunched plans.