

Agent Boundary Card

Purpose

Allowed automatically

-

Approval required

-

Forbidden

-

Allowed data

-

Forbidden/sensitive data

-

Stop conditions

- missing required data
- out of scope
- tool permission error
- conflicting authoritative sources
- external write requires approval
- max step limit reached

Success criteria

-