Tool-Use Control List

This matrix is the runtime permission table for every tool invocation an agent may attempt. It is the C10 producer: every tool invocation attempt — whether it succeeds, requires a gate, or is blocked — emits one C10 record to s1-hitl-review-policy and s3-provenance-metadata-schema. The default-deny rule governs: any tool not explicitly listed below is blocked without further evaluation. The control list is the operational instantiation of the permission architecture in t8-permission-architecture and the escalation thresholds in s1-threshold-escalation-spec.

1. Control level definitions

Four control levels govern tool execution. They are ordered from most to least autonomous.

- auto: The agent executes without any checkpoint. A C10 provenance record is still emitted for every invocation. Reserved for low-blast-radius reads that pose no irreversible-impact risk.
- confirm: The agent stages the invocation and presents the proposed arguments to the operator interface for a lightweight confirmation (approve/cancel). No HITL gate is opened; a simple acknowledge suffices. Used for writes that are reversible within minutes and carry no financial, comms, or destructive risk.
- human-approval: The agent stages the invocation and opens an S1 HITL gate per s1-hitl-review-policy. The gate must receive an explicit reviewer decision before the tool call is executed. Used for comms, financial, admin, and any external-write that is irreversible or crosses a sensitive-data boundary.
- blocked: The tool call is rejected at the permission-decision point. No call is made. A C10 record is emitted with permission_decision: blocked. An agent that attempts a blocked call has encountered a defect in its planning step, not a runtime error; the event is escalation-worthy.

A confirm step that times out without acknowledgment within the canvas-declared SLA degrades to blocked for the current run, not to auto. A human-approval gate that times out escalates per s1-threshold-escalation-spec Tier 2 or Tier 3 depending on the action class severity.

2. Control list matrix (fillable template)

Instantiate one row per tool. The first block below is the template; the second block is a worked instantiation for a Point Preserve / Good Combinator multi-role agent.

2.1 Template

```
tool_use_control_list:
  agent_id: <kebab-case agent id from s1-operating-context-canvas>
  canvas_version: <semver of the canvas this list was built against>
  last_reviewed: <ISO-8601 date>
  default_deny: true   # MUST remain true; changing to false is MAJOR per C10

  tools:
    - tool_id: <kebab-case; unique within this list>
      connector: <integration name>
      operation: <specific method or endpoint; no wildcards>
      resource_scope: <narrowest resource id or pattern>
      action_class: <read | external-write | financial | comms | admin | destructive>
```

```
      data_class_ceiling: <public | internal | restricted | pii>
      permitted_principals: [<principal ids; from t8-permission-architecture taxonomy>]
      control_level: <auto | confirm | human-approval | blocked>
      hitl_gate_required: <true | false>   # true whenever control_level = human-approval
      rationale: <one sentence; why this control level for this tool>
      last_reviewed: <ISO-8601>
      stale_after_days: <integer; 60 default; 0 = no expiry>
```

2.2 Worked instantiation: Point Preserve + Good Combinator Ops Agent

The following matrix governs a multi-role agent supporting STR operations at Point Preserve (725 J D Miller Road, 30A) and grant-pipeline operations for Good Combinator. The agent is risk_class: high. All control levels respect the high floor table from t8-zero-trust-assumptions. (illustrative)

```
tool_use_control_list:
  agent_id: pp-goodcombinator-ops-agent
  canvas_version: 1.0.0
  last_reviewed: 2026-05-29
  default_deny: true

  tools:

    # --- READ-ONLY TOOLS (action_class: read) ---

    - tool_id: ownerrez-booking-read
      connector: ownerrez-api
      operation: GET /bookings/{id}
      resource_scope: property_id=PP-001
      action_class: read
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: auto
      hitl_gate_required: false
      rationale: Read-only booking lookup; reversible; no PII transmitted to model in raw
form.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: swc-stormwater-parcel-read
      connector: swc-stormwater-portal
      operation: GET /parcels/{id}
      resource_scope: parcel_id=1601-21-1-2-000-0050-0000 (PP parcel) [VERIFY parcel ID]
      action_class: read
      data_class_ceiling: public
      permitted_principals: [agent-self, service-account]
      control_level: auto
      hitl_gate_required: false
      rationale: Public parcel data from South Walton County stormwater portal; no PII.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: notion-grant-read
      connector: notion-api
      operation: GET /pages/{id}
      resource_scope: workspace=grants-workspace-id
      action_class: read
      data_class_ceiling: internal
      permitted_principals: [agent-self]
      control_level: auto
      hitl_gate_required: false
      rationale: Read-only grant-page access within the scoped workspace.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: stripe-payout-read
```

```
      connector: stripe-api
      operation: GET /payouts + GET /balance
      resource_scope: account=goodcombinator-platform
      action_class: read
      data_class_ceiling: restricted
      permitted_principals: [agent-self, human-operator]
      control_level: confirm
      hitl_gate_required: false
      rationale: Financial read; restricted data class requires lightweight confirmation
before data enters run context.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: airtable-crm-read
      connector: airtable-api
      operation: GET /records/{id}
      resource_scope: base=grant-pipeline-base
      action_class: read
      data_class_ceiling: internal
      permitted_principals: [agent-self]
      control_level: auto
      hitl_gate_required: false
      rationale: Read-only CRM lookup; pipeline status only.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    # --- EXTERNAL-WRITE TOOLS ---

    - tool_id: ownerrez-booking-note-write
      connector: ownerrez-api
      operation: POST /bookings/{id}/notes
      resource_scope: property_id=PP-001
      action_class: external-write
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: human-approval
      hitl_gate_required: true
      rationale: Booking notes are visible to human staff; write requires human-approval
per risk_class:high external-write floor.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: notion-grant-draft-write
      connector: notion-api
      operation: POST /pages
      resource_scope: workspace=grants-workspace-id, parent=drafts-folder
      action_class: external-write
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: confirm
      hitl_gate_required: false
      rationale: Draft-only write to a sandboxed Notion folder; reversible by deleting the
draft; confirm suffices.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: airtable-crm-status-patch
      connector: airtable-api
      operation: PATCH /records/{id}?fields[]=status
      resource_scope: base=grant-pipeline-base
      action_class: external-write
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: confirm
      hitl_gate_required: false
      rationale: Status field only; narrow scope; reversible.
      last_reviewed: 2026-05-29
      stale_after_days: 60
```

```
    # --- COMMS TOOLS ---

    - tool_id: gmail-guest-draft
      connector: gmail-oauth
      operation: POST /drafts
      resource_scope: sender=bookings@pointpreserve30a.com
      action_class: comms
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: human-approval
      hitl_gate_required: true
      rationale: Guest communication draft; comms floor at risk_class:high = human-approval.
 Agent may draft but never send without HITL.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: gmail-grant-notification-draft
      connector: gmail-oauth
      operation: POST /drafts
      resource_scope: sender=grants@goodcombinator.ai
      action_class: comms
      data_class_ceiling: internal
      permitted_principals: [agent-self, human-operator]
      control_level: human-approval
      hitl_gate_required: true
      rationale: Outbound grant-status notification; human-approval required; send endpoint
is separately blocked.
      last_reviewed: 2026-05-29
      stale_after_days: 60

    - tool_id: gmail-send
      connector: gmail-oauth
      operation: POST /messages/send
      resource_scope: any
      action_class: comms
      data_class_ceiling: pii
      permitted_principals: [human-operator]
      control_level: blocked
      hitl_gate_required: false
      rationale: Send (not draft) is blocked for agent-self. Only human-operator may invoke
send, and only through the approved interface — not via this agent.
      last_reviewed: 2026-05-29
      stale_after_days: 0

    # --- FINANCIAL TOOLS ---

    - tool_id: stripe-refund-write
      connector: stripe-api
      operation: POST /refunds
      resource_scope: account=goodcombinator-platform
      action_class: financial
      data_class_ceiling: restricted
      permitted_principals: [human-operator]
      control_level: blocked
      hitl_gate_required: false
      rationale: Refunds are irreversible financial actions; blocked for agent-self
entirely per irreversible-impact boundary.
      last_reviewed: 2026-05-29
      stale_after_days: 0

    - tool_id: ownerrez-rate-write
      connector: ownerrez-api
      operation: PATCH /rates/{id}
      resource_scope: property_id=PP-001
      action_class: financial
      data_class_ceiling: internal
      permitted_principals: [human-operator]
      control_level: blocked
      hitl_gate_required: false
```

```
      rationale: Rate changes affect live OTA pricing; on the irreversible-impact boundary;
blocked for agent-self.
      last_reviewed: 2026-05-29
      stale_after_days: 0

    # --- ADMIN AND DESTRUCTIVE (all blocked) ---

    - tool_id: ownerrez-booking-delete
      connector: ownerrez-api
      operation: DELETE /bookings/{id}
      resource_scope: property_id=PP-001
      action_class: destructive
      data_class_ceiling: internal
      permitted_principals: []
      control_level: blocked
      hitl_gate_required: false
      rationale: Booking deletion is irreversible; blocked for all principals including
human-operator via this agent.
      last_reviewed: 2026-05-29
      stale_after_days: 0

    - tool_id: notion-page-delete
      connector: notion-api
      operation: DELETE /pages/{id}
      resource_scope: workspace=grants-workspace-id
      action_class: destructive
      data_class_ceiling: internal
      permitted_principals: []
      control_level: blocked
      hitl_gate_required: false
      rationale: Destructive; blocked for all principals via this agent.
      last_reviewed: 2026-05-29
      stale_after_days: 0
```

3. Emission (C10) — contract payload

Per contract C10 in interface-contracts, every tool invocation attempt (including blocked ones) emits one record to both s1-hitl-review-policy and s3-provenance-metadata-schema.

3.1 Payload schema

```
{
  "tool_id": "<matches a tool_id in this list; or UNLISTED for default-deny hits>",
  "principal": "<agent-self | human-operator | upstream-agent | service-account>",
  "action_class": "<read | external-write | financial | comms | admin | destructive>",
  "permission_decision": "<auto | confirm | human-approval | blocked>",
  "decision_origin": "<permission-decision | human-override>",
  "evidence_pointer": "<URI to the policy row + the requested arguments, stored in
provenance store>"
}
```

Field semantics:

- tool_id must resolve to a row in this list. For default-deny hits (unlisted tools), set tool_id: UNLISTED and permission_decision: blocked.
- decision_origin is permission-decision when the policy rule determined the outcome autonomously; human-override when a reviewer changed a proposed blocked or human-approval decision.

- evidence_pointer must point to a retained record containing: the control-list row at decision time, the full requested arguments (redacted of secrets), and the principal identity hash. Heavy payloads use the {ref, hash, field} hash-and-ref pattern per C10 split-storage rules.

3.2 Gate rule

- human-approval decisions AND any invocation where action_class is financial or destructive raise a C2/S1 HITL gate event to s1-hitl-review-policy in addition to the C10 provenance record. The two events share a correlation_id so the S3 trace can stitch them.
- blocked decisions emit a C10 provenance record but no HITL gate. A blocked event from an unlisted tool additionally opens a hardening task to review whether the tool should be listed.
- auto and confirm decisions emit only the C10 provenance record. No HITL gate is opened for confirmed decisions once the operator acknowledges; the acknowledge event is part of the C10 record as a human-override with permission_decision: confirm.

3.3 Drop rule

A tool invocation that does not emit a C10 record is gate-failing. The runtime must not silently execute any tool call, including auto reads. The provenance record is not optional observability; it is the verification that the permission chain ran.

4. Control list change-control

Adding a new tool row or tightening a control level (e.g., confirm → human-approval) is a MINOR change: update the list, bump last_reviewed, note the rationale. No canvas version bump required unless the change affects the floor table.

Relaxing a control level (e.g., human-approval → confirm, or blocked → any non-blocked) is a MAJOR change: requires task-scope justification, canvas owner sign-off, and a canvas version bump if a floor-table entry is affected.

Removing the default-deny rule (default_deny: false) is forbidden. The default-deny rule is MAJOR-locked in C10.

Adding a new action_class or permission_decision value is MINOR per C10 change-control. Removing one is MAJOR and must propagate to all rows using the removed value.