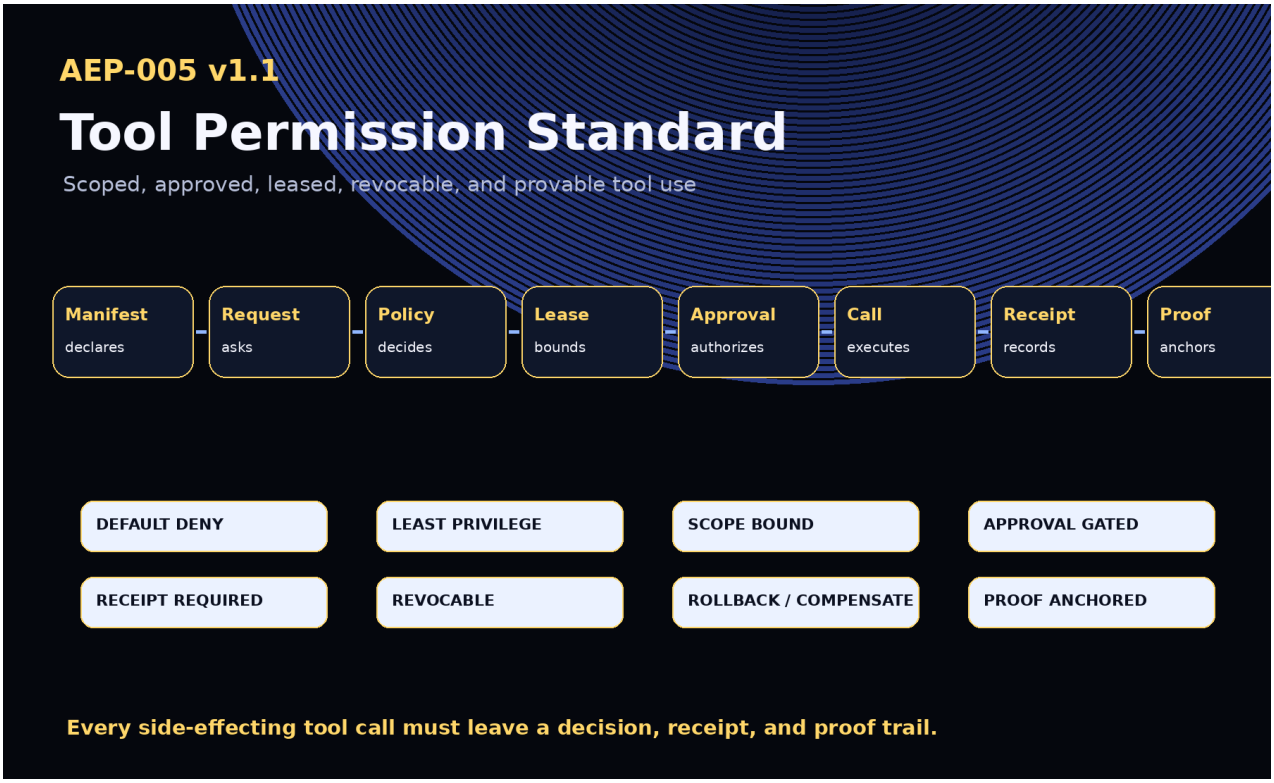
AEP-005

Tool Permission Standard

Scoped, approved, leased, revocable, and provable tool use

Version 1.1 Institutional Edition · Proof Gradient / Agent Evolution Protocol



AEP-001 defines the protocol. AEP-002 defines the docket. AEP-003 defines the packet. AEP-004 defines the gate. AEP-005 defines the permission.

1. Abstract

AEP-005 defines the Tool Permission Standard: the governance layer that determines whether an AI agent, workflow, model route, human operator, or automated system may use a tool, under what scope, for how long, with which approvals, what evidence must be recorded, and what rollback or compensation path is required.

A model may know a tool exists. An agent may request a tool. Only the Tool Gateway may authorize its use.

2. Canonical Law

No tool without permission.

No action without scope.

No high-risk tool without approval.

No side effect without receipt.

No irreversible action without rollback or compensation.

No permanent authority without expiration.

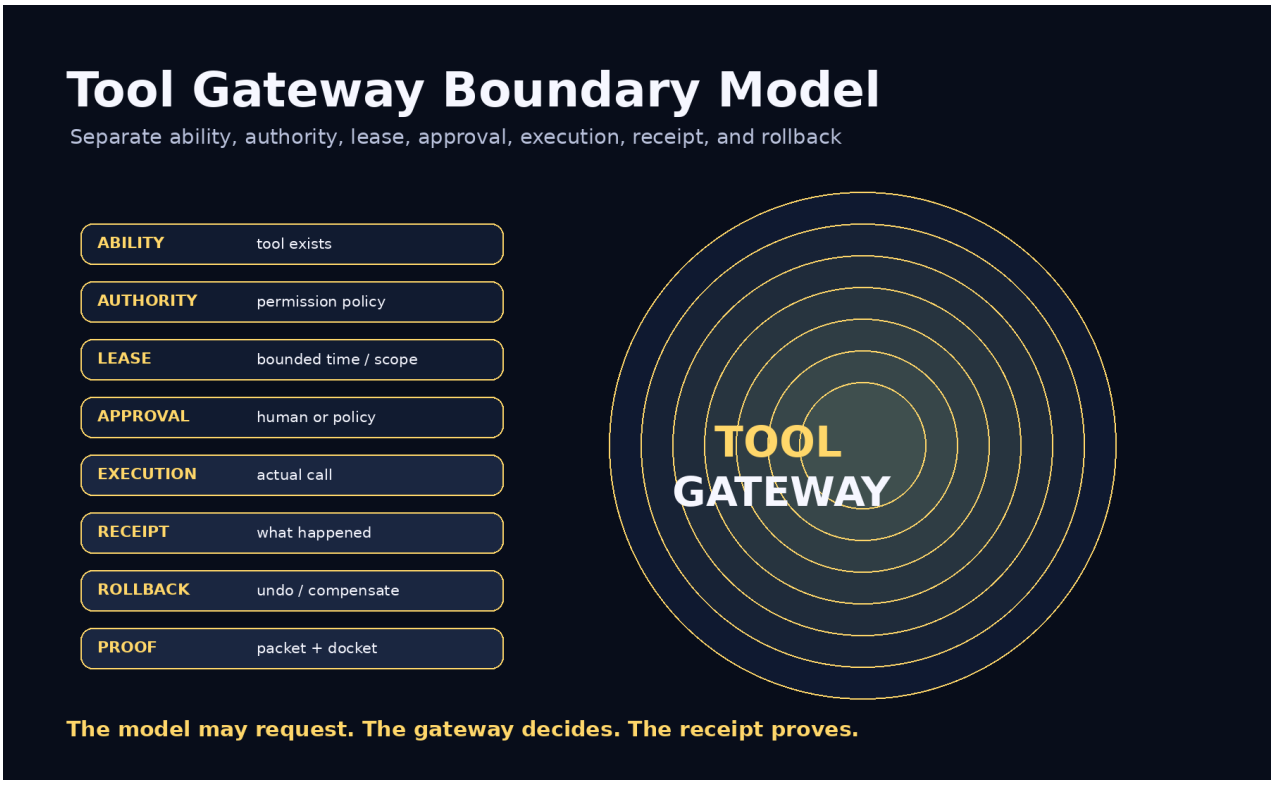
No proof, no evolution.

3. v1.1 Upgrades

- Permission leases
- Revocation receipts
- Compensation receipts
- Break-glass requests
- Data-boundary rules
- Rate-limit policies
- Separation of duties
- Tool Gateway audit tooling

4. Tool Authority Model

- Ability - the tool exists and can technically be called.
- Authority - the agent or workflow is allowed to request it.
- Scope - the permitted boundaries of use.
- Lease - the permission is time-bounded and revocable.
- Approval - human, policy, or institutional authorization.
- Execution - the actual tool call.
- Receipt - the execution result and side effects are recorded.
- Proof - the decision and receipt anchor into ProofPackets and Evidence Dockets.



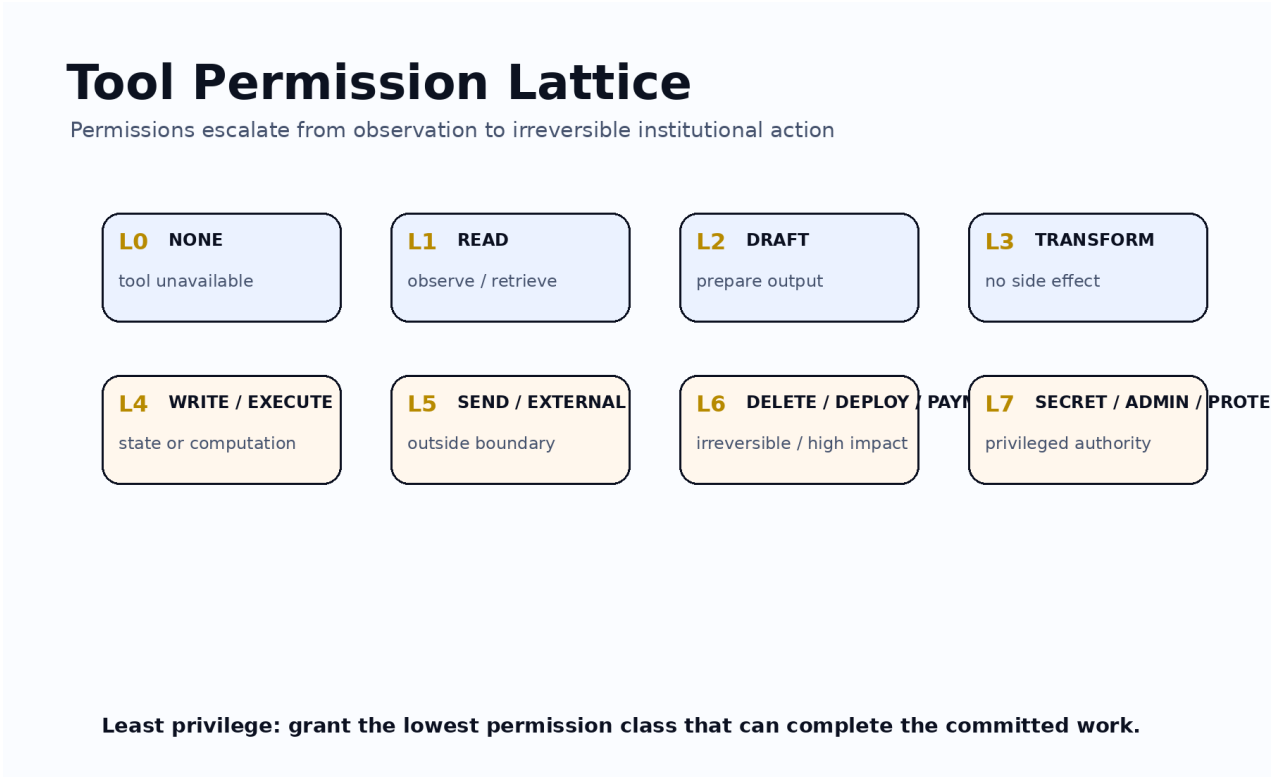
5. Permission Classes

Permission Class	Meaning
none	Tool unavailable.
read	Observe, retrieve, inspect, list, or query without changing state.
draft	Prepare output without applying it.
transform	Transform data without external side effects.
write	Change internal state or modify a system.
execute	Run code, jobs, scripts, automations, or computational tasks.
external_contact	Contact external people, systems, vendors, customers, agencies, or public endpoints.
send	Send a message, publication, email, form, API request, or external output.
delete	Delete, destroy, revoke, remove, or irreversibly alter a resource.
deploy	Release, publish, ship, merge, promote, or activate a capability.
payment	Spend money, transfer value, initiate purchase, or access payment rails.
secret_access	Read or use secrets, credentials, tokens, keys, private data, or protected evidence.
admin_change	Change permissions, roles, policies, accounts, infrastructure, routing, or governance.
protected_operation	High-impact or regulated operation requiring special authorization.
break_glass	Emergency use outside normal policy with mandatory review.

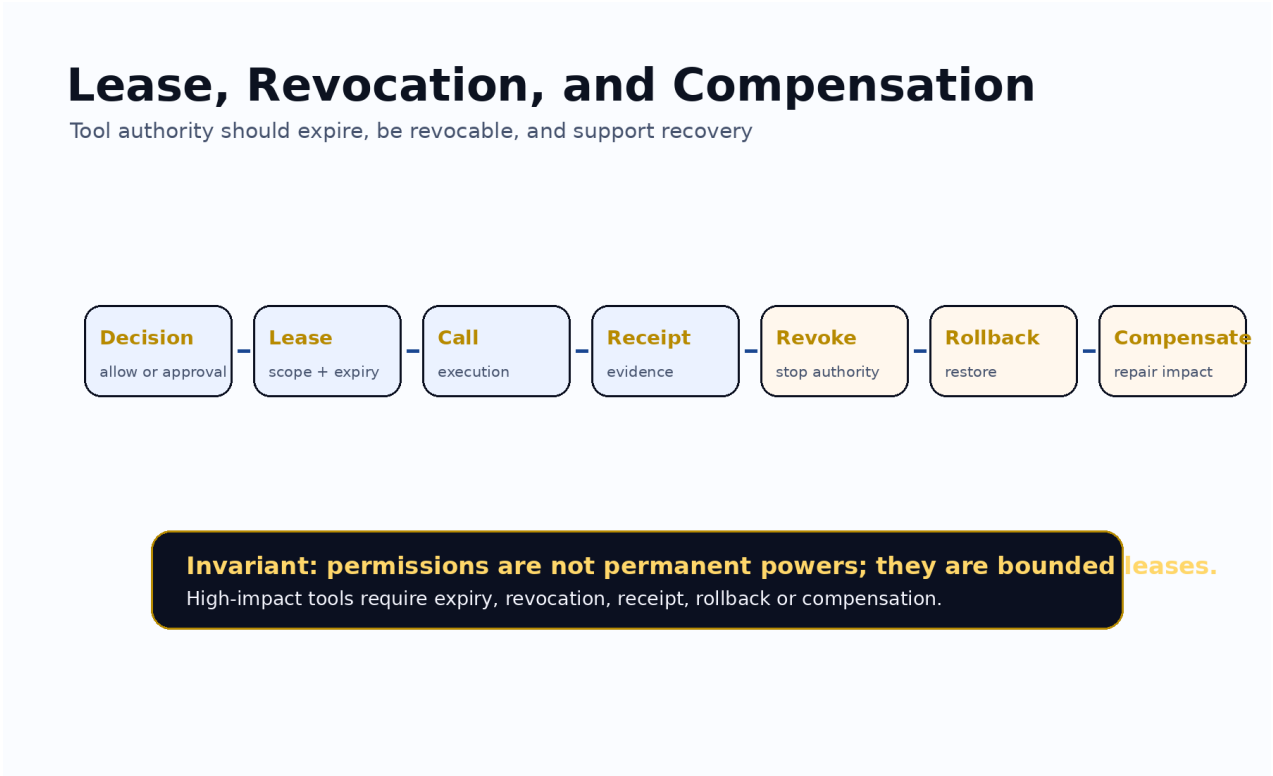
6. Core Objects

Object	Purpose
Tool Manifest	Declares tool identity, permissions, risk, data access, side effects, approval and evidence requirements.
Tool Permission Policy	Defines who may use which tools, in what scopes, with which approvals, limits, rollback and compensation.
Tool Request	Records the request before tool use.
Tool Permission Decision	Records allow, deny, approval_required, or restricted allow decisions.
Permission Lease	Records time-bounded and revocable authority.
Approval Receipt	Records human or institutional approval.
Tool Call Receipt	Records what happened after execution.
Revocation Receipt	Records termination of tool authority.
Compensation Receipt	Records remediation when rollback is impossible or insufficient.
Break-Glass Request	Records emergency use outside normal policy.

7. Permission Lattice and Lease Model



A permission is not a permanent power. It is a bounded lease. High-impact tools require expiry, revocation, receipt, rollback or compensation.



8. Default-Deny Rule

- No tool manifest exists.
- No policy applies.
- Requested class is not supported.
- Requested class is denied.
- Approval is required but absent.
- Scope is missing.
- Lease is missing or expired.
- Rollback or compensation is required but missing.
- Protected data lacks authorization.
- Budget or rate limit is exceeded.
- Separation of duties is violated.
- The gateway cannot evaluate the policy.

9. High-Risk Permission Rules

- write requires evidence, policy, scope, lease, and receipt.
- send / external_contact requires approval unless explicitly pre-authorized.
- delete requires approval, rollback or compensation plan, and receipt.
- deploy requires Selection Gate or release authority, monitoring, and rollback.
- payment requires financial authorization, budget scope, and receipt.
- secret_access requires protected access authority and evidence controls.
- admin_change requires elevated approval and separation of duties.
- break_glass requires emergency justification, temporary scope, monitoring, and post-incident review.

10. Conformance Levels

Level	Requirement
Level 0	Informal tool note.
Level 1	Tool manifest.
Level 2	Gateway decision.
Level 3	Scoped leased permission.
Level 4	Institutional permission with approval, leases, receipts, ProofPackets, rollback/compensation, revocation, and audit export.
Level 5	Sovereign / regulated permission with jurisdiction, retention, data boundary, authorized approvers, separation of duties, public/private/protected evidence boundary, institutional review, revocation, and post-incident controls.

11. Claim Boundary

AEP-005 does not claim achieved AGI, achieved ASI, perfect safety, legal compliance certification, financial or legal advice, guaranteed ROI, production readiness, government endorsement, or national-security readiness. AEP-005 defines a tool permission and proof standard.

GoalOS allows only what is scoped, approved, leased, revocable, and provable.