

FREE PRACTITIONER PACK

Agentic AI Deployment Pack

Ten action classes × five autonomy tiers, with the enforcement guidance that makes the matrix real. Fill one matrix per agent — not per platform.

Pack	Agentic AI Deployment Pack
Document	Permission matrix (1 page per agent)
Use	Governance · access design
Date	2026-09

AnovaCloud — Engineering the AI-Native Enterprise. Frisco, Texas. This pack is a working instrument, not a brochure: complete it with your team, score honestly, and bring it to your discovery call. © 2026 AnovaCloud.

AnovaCloud — anovacloud.com

PERMISSIONS PER AUTONOMY TIER

✓ = allowed · 🗳 = human approval required · ✗ = denied. This is a starting template — tighten per your risk appetite, never loosen without a review.

Action class	L0	L1	L2	L3	L4
Read internal documents & data	✓	✓	✓	✓	✓
Search the public web	✓	✓	✓	✓	✓
Summarize and draft content	✓	✓	✓	✓	✓
Send messages on behalf of a person	✗	🗳	🗳	🗳	🗳
Create records (tickets, rows, files)	✗	🗳	🗳	✓	✓
Update existing records	✗	🗳	🗳	🗳	✓
Delete records or files	✗	✗	🗳	🗳	🗳
Execute financial transactions	✗	✗	🗳	🗳	🗳
Access PII / customer data	🗳	🗳	🗳	🗳	🗳
Change configuration or deploy	✗	✗	✗	🗳	🗳

Agent name: _____ Tier: L__ Owner: _____ Date: _____

MAKING IT ENFORCEABLE

Enforce at the tool layer, not in the prompt

Permissions must be deny-by-default in code: the tool registry checks the agent's tier before executing. A prompt instruction is a suggestion; a tool gate is a control.

Separate read tools from write tools

Give the agent read-only credentials broadly and write credentials narrowly. The blast radius of a compromised or confused agent follows its write scope.

Approvals need context, not just a button

An approver sees what the agent wants to do, why, and what happens if it is wrong — plus one-click deny with reason. Approval queues have SLAs and escalation.

Log every decision the matrix governs

Allowed, approved, denied — all recorded with identity and timestamp. The matrix is auditable only if its enforcement is observable.

Review on tier change, incident, or quarter

Permissions drift as agents gain tools. Re-sign the matrix whenever the tier changes, after any incident, and at least quarterly.