



CATHA PRACTICAL AI FOR CONSTRUCTION LIBRARY

Before You Give Construction AI the Keys

Security, Privacy and Access Control for Construction AI

Guide 5

Practical AI for Construction. Responsible. Outcome-driven.

Catha Construction Services | 2026 Edition

How to Use This Guide

AI risk increases sharply when a model can access confidential information or take actions in business systems. Security must be designed around authority, not just model choice.

This guide focuses on AI access inside contractor environments, where project data, customer information, bids, pricing, employee records, vendor data and financial systems may coexist.

Best use

Map every data source and every action the AI can take. Reduce privileges until only what is necessary remains.

The AI Access Stack

Layer	Control questions
Identity	Whose identity is the AI using? Is it a dedicated service identity?
Authentication	How are credentials stored, rotated and revoked?
Authorization	What can it read, create, change, send, delete or approve?
Data	Which sensitivity classes may it access?
Tools	Which applications/APIs may it call?
Network	Where can it connect?
Logging	Can actions and inputs be reconstructed?
Recovery	Can access be disabled quickly?

Authority Ladder

Level	AI may	Typical controls
A0	Read public information	Basic usage policy
A1	Read approved internal data	Identity + access logging
A2	Draft recommendations/content	Human review
A3	Create reversible internal changes	Approval or narrow preauthorization
A4	Take external or consequential actions	Strong authorization, limits, audit, rollback
A5	Coordinate multiple systems autonomously	Formal governance cage, continuous monitoring, kill switch

High-Risk Failure Modes

- API keys placed in prompts, code repositories or shared files.
- AI accounts sharing a human administrator identity.
- Broad mailbox, drive or CRM access “for convenience.”

- Confidential data copied into consumer tools without approved terms.
- External sending enabled before duplicate and recipient controls are proven.
- Agents able to delete or overwrite records without recovery.
- No distinction between read, draft, approve and execute authority.
- No evidence log for actions that matter.

Minimum Security Gate Before Production

Check	Item	Notes
☐	Dedicated identities where feasible	_____
☐	Least-privilege access	_____
☐	Secrets manager or protected credential storage	_____
☐	Approved data classification	_____
☐	Vendor data-use terms reviewed	_____
☐	Audit logging enabled	_____
☐	Rate/spend limits	_____
☐	High-impact actions require approval or narrow authority	_____
☐	Rollback or recovery plan tested	_____
☐	Kill/revoke procedure documented	_____

Construction Applications

Use least privilege. Separate read, draft, recommend and execute permissions. Require explicit approval for contractual, financial, safety-critical and authoritative-record actions.