AI governance in the UAE: the six documents checklist

When a regulator, a client's compliance team or a procurement panel asks about your AI, they ask for documents, not principles. Tick each item when you could hand it over today. Complete one copy per legal entity.

01 An inventory of AI systems

What is deployed, what data it touches, who owns it, what it is permitted to do.

- [ ] One row per AI system, including AI features inside software you already use
- [ ] The personal data each one touches
- [ ] A named owner for each system
- [ ] What each system may do, and what it may never do
- [ ] Reviewed quarterly, with the date recorded

02 A lawful basis for each processing activity

Consent, contract or legitimate interest, recorded before processing starts, not reconstructed afterwards.

- [ ] A basis recorded for each activity, before it starts
- [ ] Training or fine-tuning treated as a separate activity
- [ ] Customers told where AI is used, and how to reach a person
- [ ] A route for people to exercise their data rights

03 An impact assessment for higher-risk uses

Anything that makes or materially influences a decision about a person.

- [ ] Higher-risk uses identified in the inventory
- [ ] An assessment written before go-live, not after
- [ ] Risks, mitigations and who signed it off
- [ ] Revisited when the system or its data changes

04 A retention position

How long prompts, outputs and logs are kept, and enforced deletion. The most overlooked data store in the estate.

- [ ] A retention period decided for prompts and outputs
- [ ] The same for logs and traces
- [ ] Deletion enforced, not just written down
- [ ] Backups and vendor-side copies included

05 A transfer record

If inference runs outside the UAE, the data in the request has crossed a border, and that needs a basis.

- [ ] Where each system's inference runs: country and region
- [ ] Whether cross-region processing is switched on
- [ ] Where logs and backups are stored
- [ ] The basis for each transfer, recorded

06 Human oversight, defined per system

Who reviews what, how often, and who can stop it.

- [ ] Who reviews the system's output, and how often
- [ ] Which actions need a person to approve: sending, paying, deleting
- [ ] Who can stop it, without a deployment
- [ ] That stop has been tested, with the date recorded

+ Which regime governs each entity

The federal PDPL, the DIFC and ADGM are separate data protection regimes with separate regulators. A group with a free zone entity and a mainland entity can answer to more than one. Health and financial data carry sector rules on top.

LEGAL ENTITY	REGIME (PDPL / DIFC / ADGM)	SECTOR RULES	WHERE ITS DATA SITS

Controls that cost almost nothing, if decided before go-live: a scoped role per agent, not a shared account · a person approving consequential actions · log retention someone decided, and enforced · the region chosen on the compliance position, not on speed · the inventory kept current · what each system must never do, written down.

The full guide, with what is different in the UAE and the common mistakes: nexuslabuae.ai/insights/ai-governance-data-privacy-uae. For staff rules, the free AI use policy template.

Free to copy and share with attribution to Nexus Labs AI (nexuslabuae.ai). This checklist is operational guidance, not legal advice; confirm which regimes apply to your structure with your own advisers.