# Module 11 – Distributed AI Execution & Evaluation Scaffold

Module ID: AI-EXEC-011

Version: 4.1 (Revised CTO Edition)

Layer: AI Containment & Trust Layer

Status: RELEASE

Dependencies: Module 00, Module 06, Module 12

## 0. Purpose & Enforcement Point

This module defines the distributed AI execution and model evaluation control layer for MaxOneOpen v4.1. It ensures that all AI model activities are trust-classified, manifest-declared, session-capsuled, and traceable across nodes. All executions are runtime-bound, evaluation-controlled, and capsule-recorded for forensic inspection.

## 1. AI Invocation, Manifest Binding & Execution Protocol

Each AI execution is triggered via `AI\_EXECUTE()`:  
- `model\_id`, `input\_context`, `trust\_class`, `manifest\_id`  
Only models that:  
- are declared via Manifest Capsule (Module 06),  
- pass trust validation (Module 12), and  
- have role-scope approval (Module 03)  
may execute. Output and trace are bound to an `AI Execution Capsule (AIEC)`.

## 2. Evaluation Scaffold, Metrics & Result Anchoring

Each execution is coupled to an evaluation scaffold, which:  
- verifies consistency, explainability and trust zone limits  
- evaluates result deviation and bounded behavior compliance  
- produces a `Model Evaluation Capsule (MEC)`:  
`{ model\_id, input\_ref, evaluation\_result, deviation\_score, trust\_flags, timestamp }`  
Capsules are committed via Module 13 and reviewed in Module 14.

## 3. Distributed Execution Logic & Containment Enforcement

Distributed model execution is governed by:  
- node eligibility (must match trust classification)  
- IO relay via scoped Twin Messaging (Module 09)  
- capsule linkage to fork-safe ledger states  
Execution is sandboxed (Module 07) and cannot persist state, spawn uncontrolled subprocesses or modify its runtime outside declared scope.

## 4. Capsules & AI Forensic Artifacts

Artifacts per execution:  
- `AI Execution Capsule (AIEC)` – `{ exec\_id, model\_id, input\_hash, trust\_class, output\_hash, timestamp }`  
- `Model Evaluation Capsule (MEC)` – see above  
- `Violation Capsule (VC)` – on trust breach, policy deviation, or output manipulation  
All events are ledger-committed and visible to certified forensic roles.

## 5. Intermodular Bindings & Evaluation Hooks

This module connects to:  
- Module 06 (Manifest Engine) for model declaration  
- Module 07 (Sandbox) for execution isolation  
- Module 09 (Twin Messaging) for scoped IO routing  
- Module 12 (Trust Enforcement) for trust classification  
- Module 13 (LedgerSync) for result anchoring  
- Module 14 (Audit Capsule) for trace validation

## CTO Validation Matrix

Module 11 (CTO Edition) guarantees the following verifiable conditions:  
- All AI models are manifest-declared, trust-classified, and traceable: YES  
- Executions are sandboxed and output-bounded: YES  
- Evaluation capsules record behavior, metrics, and compliance: YES  
- AI cannot persist or self-replicate across sessions: YES  
- Ledger traceability and audit access is guaranteed: YES