# Module XX – Runtime Isolation & Security Capsule

Version: 4.1 | Classification: CTO Mandatory (Execution Safety & Trust Boundary Enforcement)

Scope: Isolation model, memory boundaries, trust-layer execution contract

## 0. Purpose & Security Relevance

This module defines the runtime execution boundaries and security enforcement logic for MaxOneOpen v4.1. It formalizes how execution environments, memory access, and policy injection are isolated from core ledger operations, ensuring deterministic and trust-scoped capsule behavior. The contract separates sandboxed operations from sovereign capsule flows and enforces tier-based trust checks.

## 1. Execution Isolation Model

- Tier 5 entities must execute in sealed sandbox runtime  
- Execution Capsule (EC) must not access ledger memory directly  
- All capsule validation occurs outside execution host via capsule verifier  
- Rule injection occurs via shared pipe, not API binding  
- Fork or replay detection modules must not run in same namespace as execution logic

## 2. Trust Boundary Contract (Capsule Enforcement)

- Trust Tier < 2 cannot commit certification or audit-impacting capsules  
- Only Tier 1 can inject FAC, FCC, CCC  
- Sandbox runtimes may read policy scope, but cannot alter capsule lineage  
- Capsule Verifier runs in immutable memory space (read-only)  
- Capsule violation (e.g. unauthorized write, skipped hash) → triggers Trust Violation Capsule (TVC)

## 3. Security Anchors & Runtime Design

- Use of ephemeral memory blocks for rule interpretation  
- Pre-execution signature inspection and hash-lock verification  
- Separation of policy engine and execution pipeline  
- Prevention of capsule chain traversal outside declared scope

## 4. Isolation Enforcement Diagram (non-code)

System zones:  
[Sandbox Execution Host] ←| pipe |→ [Verifier Engine] ←| ledger chain |→ [Audit / Federation Logic]

## 5. Failure Triggers & Security Breach Handling

- On runtime memory access breach → sandbox is frozen  
- On invalid signature → EC capsule marked untrusted  
- On cross-tier capsule emission → Alert Capsule (TVC + PCC) emitted  
- Ledger lock applies until recovery (see Recovery Simulation Capsule)