# Module XX – Default Trust Tier Profile & Role Enforcement Matrix

Version: 4.1 | Classification: CTO Mandatory (Trust Tier Standardization)

Scope: Operational role tiers, capsule permissions, runtime execution boundaries

## 0. Purpose & Tiering Enforcement Logic

This module defines the standardized trust tier hierarchy, enforcement boundaries, role capabilities, and capsule interaction scope for MaxOneOpen v4.1. It enables consistent execution policy, certification scoring, capsule injection filtering, and trust downgrade logic. Tier definitions are mandatory for all runtime, simulation, audit, and policy modules.

## 1. Tier Overview & Enforcement Matrix

Tier 0 – Root Sovereign Authority  
- Defines GCL, FAC, FCC and owns signature root  
- Cannot be delegated or auto-escalated  
  
Tier 1 – Ledger & Capsule Sign Authority  
- Commits all capsules to the ledger  
- May sign REC, CCC, RFC, SCC, FAC, FRC  
- Must be traceable to Tier 0  
  
Tier 2 – Audit & Simulation Role  
- Executes capsule replay checks, alert trace evaluation  
- May inject GRCC, ASC, VSC capsules  
- Read-only access to capsule scope ≥3  
  
Tier 3 – Policy Agents & Rule Enforcers  
- Executes rule logic and triggers alerts  
- May propose policies, not sign them  
- Can trigger PCC, ALR, RAC capsules  
  
Tier 4 – Operational Observer or Add-on Controller  
- Reads manifest, runtime alerts, trust overlays  
- May submit FCC requests (reviewed by Tier 1)  
- Cannot interact with capsule stream directly  
  
Tier 5 – Sandbox Entity / Non-Trusted Extension  
- Executable only in sandbox scope  
- Cannot emit capsules or perform runtime effects  
- Always trace-bound to Tier 3+ parent

## 2. Tier Drift Control & Violation Handling

Any capsule or action performed above declared tier triggers:  
- `Trust Violation Capsule (TVC)`  
- audit suspension  
- policy freeze or isolation mode  
Auto-escalation is disabled by design. Only Tier 0 may reassign tiers.

## 3. Certification Enforcement & Score Dependency

Tier definitions affect:  
- simulation coverage range  
- capsule integrity scope  
- trust downgrade paths  
- federation approval logic  
Module 17 certification requires traceable tier assignments per actor.