MaxBridge v1.2 – System Module 03

Module Title: Policy Enforcement & Rule Prioritization

Version: 1.2

Document Type: System Core Module

License: TBYD License v2.2 + Addendum A (Preview Right Only)

Subsystem: MaxBridge (Compatibility & Control Layer)

Release Context: Part of MaxOneOpen v4.1 ecosystem – standalone deployable

Status: CTO-aligned – certified structure

# 1. Purpose

This module defines how MaxBridge applies, enforces and prioritizes structural rules and external policies during capsule validation. All permission, rejection or override decisions are driven by signed rule sets originating from MaxOneOpen governance or MaxReg execution layers.

# 2. Rule Types and Sources

MaxBridge distinguishes between multiple policy and rule types:

* - Capsule Policy: Defined within the capsule manifest
* - System Rule: Inherited from MaxOneOpen's core architecture layer
* - Execution Override: Derived from MaxReg or escalated MaxTune context
* - Emergency Directive: Injected manually or via Treaties (e.g., cost, legal breach)

# 3. Rule Execution Priority

MaxBridge applies strict rule prioritization. In case of conflict, precedence is determined as follows:

1. 1. Emergency Directive (highest – overrides all)
2. 2. MaxReg System Rule
3. 3. MaxOneOpen Architectural Policy
4. 4. Capsule Policy (applied only if compliant)

# 4. Enforcement Mechanics

Rules are executed through structural validation checks, not runtime logic. Each capsule must pass an integrity scan that matches its rule scope, declared license, audit flags and intended operation. Partial matches are forbidden. Any policy collision results in capsule quarantine or breach signaling.

# 5. Role of MaxReg

MaxReg provides the executable logic tree for rule enforcement. All dynamic conditions (e.g., quota, time, fork depth) are calculated by MaxReg and injected into MaxBridge through signed execution packages. This prevents MaxBridge from making standalone decisions.

# 6. Escalation & Breach Signaling

Any enforcement failure is relayed to MaxAudit for breach anchoring and optionally forwarded to external Treaty parties. Policy override attempts are logged, signed, and retained for future dispute validation.