

## **MaxOps – Structural Use Case Playbook for Forking & Audit Paths**

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Purpose**

This playbook introduces exemplary structural workflows in MaxAudit-based infrastructures. It provides role-based walkthroughs of key actions such as forking, auditing, disclosure, and recovery—ideal for training, workshops, and onboarding.

### **2. Format & Usage**

- Each use case includes:
  - Context and role (e.g., Operator, Regulator)
  - Step-by-step structural events
  - AuditChain and registry impact
  - Optional variation paths
- Use cases are generic and reproducible offline

### **3. Use Case A – Fork Registration by Operator**

- ◆ Role: Operator
- ◆ Action: Creates a custom instance variant (fork)
- ◆ Steps:
  1. Modify MaxInstance structure in Fork Editor
  2. Export signed Fork Profile
  3. Submit via airgapped registry upload
  4. Receive Fork ID + public anchor hash
  5. Use in all future audits

### **4. Use Case B – Yellow Audit & Remediation Flow**

- ◆ Role: Operator + Regulator
- ◆ Trigger: Audit detects structural deviation (level 1–2)
- ◆ Steps:
  1. Yellow status appears in Verifier output
  2. System enters remediation window (configurable, default: 10 days)
  3. Operator applies fix and re-runs audit
  4. If green, certification chain continues
  5. If red, system suspended and flagged

## 5. Use Case C – Dongle Trigger & Emergency Shutdown

- ◆ Role: Regulator
- ◆ Context: Dongle inserted on site without notice
- ◆ Steps:
  1. Dongle runs airgapped audit ( $\approx 4$  min)
  2. Red result detected (tamper/fork mismatch)
  3. MaxControl triggers shutdown policy
  4. Audit logged and signed
  5. Incident escalation via predefined channel

## 6. Use Case D – Public Verification via PoS API

- ◆ Role: Customer or Partner
- ◆ Goal: Check system trust state without disclosure
- ◆ Steps:
  1. Scan QR / submit Fork ID to PoS endpoint
  2. Receive verification status (true/false, green/yellow/red)
  3. Optional download of audit proof
  4. Trust layer integrates into external CI or procurement process