

## **MaxAudit Dongle Operation & Regulatory Visit Protocol**

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Purpose of the Dongle**

The Dongle is a state-operated audit device designed to verify the structural compliance of a running MaxOne system. It provides non-invasive, air-gapped, cryptographically verifiable inspections without requiring system shutdown, user interaction, or internet access.

### **2. Operating Characteristics**

- No dependency on host system software
- Operates in read-only mode
- No data transmission or storage
- Generates signed audit result locally
- Stateless across visits
- Inspection duration:  $\leq 4$  minutes under standard load conditions

### **3. Plug-In Procedure**

1. Inspector inserts Dongle into designated audit interface (USB/serial)
2. Dongle auto-executes verification against on-device schema
3. Traffic light status is shown immediately (Green / Yellow / Red)
4. Audit protocol is generated and can be printed/exported
5. Dongle can be removed directly after result display

### **4. Regulatory Visit Protocol**

All visits by regulatory authorities using the Dongle follow the standardized MaxAudit Visit Protocol:

- Visits are unannounced and may occur at any time
- Inspectors require no administrative access
- Operator presence is not required for audit
- No advance notice, no post-audit negotiation
- Failure to cooperate results in system blacklisting

### **5. Result Handling**

- Green: Visit completed, no further action
- Yellow: Operator must fix issue and request re-audit within 10 days

- Red: Regulator is authorized to deactivate system immediately and escalate
- All results are logged cryptographically and anchorable

## **6. Tamper Protection**

The Dongle uses tamper-evident firmware, physical shielding, and cryptographic attestation to protect against reverse engineering, spoofing, or manipulation. Any deviation from its certified state results in self-deactivation and alert signal.

## **7. Certificate Binding**

Every Dongle is bound to a public MaxAudit Inspector Certificate. Verification of audit results is only valid if signed by a registered Dongle instance. Certificates are updated annually via offline authorization process.