

## **MaxAudit – Airgap Audit Deployment Protocol**

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Purpose**

This document defines the standard protocol for conducting MaxAudit audits in fully airgapped environments. It provides a secure and reproducible methodology for verifying system integrity without requiring any network access or external connectivity.

### **2. Supported Environments**

- Critical infrastructure zones (CNI, SCADA, etc.)
- Military or classified networks
- Industrial control systems (ICS)
- High-security labs or sovereign compute enclaves

### **3. Deployment Method**

- Dongle or Verifier is preloaded with signed audit schema
- Operator initiates offline scan on target system
- All evaluation runs entirely in memory, no disk writes
- Results are exported via USB, QR, or printout as signed audit proof

### **4. Import/Export Interfaces**

- Acceptable import media: write-once USB, optical disc, encrypted SD card
- Acceptable export methods:
  - JSON result file on airgap-certified device
  - PDF or printed audit report
  - QR snapshot (offline readable, signed hash)
- Output must include:
  - Timestamp, audit signature, system hash, Fork ID

### **5. Validation Path**

- Audit results are validated externally against reference schema
- Fork Registry may be mirrored on local secure storage
- License verification occurs using embedded signature set
- Full certification chain must be reproducible without online lookup

## 6. Security Considerations

- No outbound connectivity permitted
- Dongle self-verifies firmware state before execution
- All exports signed locally and non-editable
- No result upload permitted unless reconnected to validation network

## 7. Operational Roles

- Operator: initiates audit run, extracts result
- Auditor: validates structure externally
- Governance body: confirms signature integrity, anchors result if valid