

# **MaxOps – Vulnerability Handling & Structural Disclosure Protocol**

Version: 1.0

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

License: MaxOneOpen License v2.2 – Structurally Enforced

## **1. Purpose**

This protocol defines the standard process for disclosing, evaluating, and resolving structural vulnerabilities within MaxAudit-based systems. It provides a secure, verifiable path for DevSecOps teams, operators, and researchers to coordinate remediation without compromising structural integrity.

## **2. Scope of Applicable Vulnerabilities**

- Fork bypass logic or incorrect audit interpretation
- Broken audit signature chain or revoked license state
- Unauthorized audit suppression or redirection
- MaxInstance configuration bypass
- Verifier injection or tamper detection failure

## **3. Disclosure Channels**

- Primary: Signed report via offline registry submission (airgap method)
- Optional: GPG-encrypted email to SAC Audit Response Team
- Optional: Tokenized Fork alert via internal Fork Registry hook

## **4. Process Flow**

1. Vulnerability detected by operator, dev team, or third party
2. Submit signed report to SAC (preferred: airgap + offline verification file)
3. SAC triage assigns structural class (1–4 severity)
4. Optional Fork suspension or audit freeze
5. Fix issued as patch, schema update, or registry directive
6. Fix tested against regression audit and published

## **5. Roles & Responsibilities**

- Operator: Detection, temporary containment
- SAC: Classification, integrity evaluation, countermeasure design
- Registry: If required, initiate trust freeze or anchor revocation
- Verifier/Dongle: No automatic mitigation unless registry confirms patch

## **6. Incentive Models (Optional)**

- Structural bounty offered for severity 3–4 vulnerabilities
- Fork-level bonus if fix is submitted alongside proof-of-concept
- Rewards paid via structural contribution token (SCT), not monetary

## **7. Public Disclosure Policy**

- All accepted vulnerabilities are archived and publicly hash-anchored
- Redacted audit traces may be shared for transparency
- System names, operators, or configurations remain pseudonymized