

v3.4-STO-003 – Object Lifecycle, Snapshot Control & Retention Policy

Document Title	Object Lifecycle, Snapshot Control & Retention Policy
Version	v3.4
Document ID	v3.4-STO-003
Date	2025-03-22
Author	Take Back Your Data – Storage Lifecycle Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the object lifecycle management, snapshot logic and retention rules in MaxOneOpen. It ensures that all data objects are bound to strict, user-controlled and cryptographically enforced timelines and visibility.

2. Object Lifecycle States

- States: Created → Sealed → Accessed → Snapshotted → Expired → Deleted
- Transitions must be logged and optionally notarized
- Each object carries lifecycle metadata, bound to schema + context

3. Snapshot Management

Snapshot Type	Trigger	Storage Rule
Manual Snapshot	User-signed runtime trigger	Encrypted + versioned vault
Runtime Mirror	Twin-defined state capture	Temporary, volatile
Archive Seal	Export action with context	Immutable + hash verified
Emergency Dump	Control override	Time-locked, revocation-bound

4. Retention Policy Engine

- Policies defined per object schema
- Forks must enforce TTL, trigger and retention class
- Deletion must zero object and metadata without cloud fallback
- All expired data must leave a hashed proof of deletion

5. Certification Impact

- Certification requires object state traceability
- Snapshot logs must be exportable and verifiable
- Forks must expose object policy map + runtime enforcement trigger
- No rollback may occur after final state unless via signed exception

6. Certification Relevance

MaxOneOpen deployments must guarantee object lifecycle traceability, user-bound snapshot logic and hard retention limits. Forks without enforceable object management will lose certification.