

## v3.4-STK-007 – Secure Memory & Local Data Isolation

Document Title	Secure Memory & Local Data Isolation
Version	v3.4
Document ID	v3.4-STK-007
Date	2025-03-22
Author	Take Back Your Data – Security & Memory Unit
Document Type	Public / Certification / Internal

### 1. Purpose & Scope

This document defines the technical foundations for secure memory handling and strict local data isolation in MaxOneOpen. It ensures that all inference and interaction operations comply with UDUH (User Data in User Hands) and Zero-Knowledge principles.

### 2. Secure Memory Zones

- Memory is partitioned into isolated zones per task/twin
- Access to each zone is cryptographically scoped
- Memory is ephemeral and self-destructs on task termination
- Zones are hardware-assisted (e.g. TEE, SGX, SEV, RISC-V PMP)

### 3. Local Storage Constraints

- Persistent storage is opt-in and user-controlled
- No default logging of inputs, prompts or context
- Local write operations must be encrypted and scoped
- Audit hash required for any local data persistence
- Ephemeral memory takes precedence unless overridden by user policy

### 4. Data Isolation Enforcement

Mechanism	Function	Isolation Level
Twin Memory Walls	Runtime-isolated memory zones per twin	Process-level
Context Masking	Selective exposure of prompt context	Task-level
Shadow Copies	Clone-on-read memory isolation	User-level
Hash Verification	ZKP-style proof of access boundary	Cryptographic

### 5. Compliance Constraints

- No memory sharing between twins unless explicitly defined
- All memory and storage must be scoped by policy
- Forks must declare memory architecture and access rules
- Zero-knowledge compliance must be auditable via trace logs

## 6. Certification Relevance

Secure memory and local isolation logic are core requirements for MaxOneOpen certification. Deployments must verify that no central memory exposure, shadow logging or policy breach is possible under standard operation.