# Automated Local Profile Lifecycle Management Standard

**Introduction**
The primary objective of this standard is to fortify the organization's security posture by minimizing the lateral movement risk associated with dormant user credentials. By automating the removal of inactive profiles, ensuring optimal system performance, the agency reclaims localized storage capacity and maintains a "clean state" environment on shared or assigned assets.

**Purpose**
This standard is mandatory and applies to all managed Windows workstations, laptops, mobile devices and remote endpoints owned. It encompasses all user-level profiles created during local authentication, regardless of the employee's department or physical location.

**Definitions**
CSP – configuration service provider.

Dormant user credentials – accounts still active in a system but not used for an agreed period (e.g., 30-90+ days) and are no longer tied to an active employee or workload.

**Standard**
Retention standard.

- The organization mandates a 60-day inactivity threshold for all local user profiles. Any profile that has not recorded a successful interactive login for a period of 60 consecutive days is deemed "stale" and is subject to immediate, automated purge from the local disk.

Technical implementation (Intune/MDM).

- Enforcement is managed globally via Microsoft Intune using the user profile configuration service provider (CSP).

Automation – The "Delete user profiles older than a specified number of days on system restart" setting is set to 60.

- Execution: The system evaluates profile age during the boot cycle; profiles meeting the age criteria are deleted in their entirety (including the C:\Users\directory and associated registry hives).
- Verification: Intune reporting is used to audit compliance and ensure the policy is successfully pushed to all enrolled endpoints.

User responsibility and data integrity.

- This standard reinforces the "cloud-first" data strategy. Employees are strictly prohibited from storing sole copies of business-critical data within local-only profile folders. All work must be synced to OneDrive for Business or SharePoint to ensure data persistence after a profile is purged. OMES is not responsible for the recovery of locally stored data deleted under this standard.

**Compliance**
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

**Rationale**
To ensure efficient, secure, and cost-effective delivery of essential public services, all state agency IT purchases and projects must receive central approval. This allows the Chief Information Officer to evaluate agency needs and capabilities, strengthen data protection and security, and streamline and consolidate systems to reduce costs for taxpayers.

**References**
- Section is optional. Delete if not used.

**Revision history**
This standard is subject to periodic review to ensure relevancy.

| | |
|---|---|
| **Effective date:** 05/26/2026 | **Review cycle:** Annual |
| **Last revised:** 05/26/2026 | **Last reviewed:** 05/26/2026 |
| **Approved by:** Dan Cronin, Chief Information Officer | |