

Number:	03.1.4	Page:	1 of 3
Latest Version:	1.1	Revision Date:	08/04/2016
Effective Date:	08/04/2016	Replaces:	1.0
Revised By:	Joshua Graves	Review Cycle/Date:	Annual
Reviewed By:	Laquetta Russell	Reviewing Unit:	Security Provisioning
Title:	Active Directory Identity Management SOP		
Description:	This document is the operating standard for Identity Management for Active Directory.		

Active Directory Identity Management Standard Operating Procedure

1. General Statement of Purpose
 - 1.1. This document defines the Identity Management procedures for Active Directory.
2. Scope
 - 2.1. This document applies to all state of Oklahoma employees that use Active Directory.
3. Discipline
 - 3.1. Security & Compliance Standards
4. Terms and Definitions
 - 4.1. Employee – Worker who is economically dependent on the business of the employer.
 - 4.2. Contractor – Worker with economic independence who is in business for themselves.
 - 4.3. User ID – A unique login ID assigned to each user of State Systems.
 - 4.4. Decentralized Security Representative (DSR) – An individual, designated by the head of the agency, who is authorized to submit requests for the creation of new User IDs, modification of user access or termination of user access.
 - 4.5. Disabled account – An inactive account requiring approval from an agency’s Decentralized Security Representative to enable.
 - 4.6. Locked out account – An account that is blocked from user access and requires the OMES Service Desk to unlock. (Examples that may cause this include password expiration or a user incorrectly entering a password too many times.)
5. Discussion
 - 5.1. OMES IS ensures that all users (internal, external and temporary) and their activity on IT systems are uniquely identifiable and that access is established through an authentication mechanism. There is also a process for identifying and suspending inactive accounts.
 - 5.1.1. All users of State Systems have a uniquely identifiable user account. Generic accounts are not permitted without explicit exception review and authorization from the Chief Information Security Officer and the applicable System or Data Owners. Generic accounts have additional controls in place for accountability and a periodic review for their applicability.
 - 5.1.2. All user accounts not using the system for a period of 60 days are automatically disabled by OMES IS. Restoration of the user account must be authorized by the user’s management or the agency’s Decentralized Security Representative (DSR) via CRM Case.

Number:	03.1.4	Page:	2 of 3
Latest Version:	1.1	Revision Date:	08/04/2016
Effective Date:	08/04/2016	Replaces:	1.0
Revised By:	Joshua Graves	Review Cycle/Date:	Annual
Reviewed By:	Laquetta Russell	Reviewing Unit:	Security Provisioning
Title:	Active Directory Identity Management SOP		
Description:	This document is the operating standard for Identity Management for Active Directory.		

5.2. Access Control

- 5.2.1. Access for all new OMES employees is requested as part of the Onboarding process. Refer to **02.3.1 Onboarding**.
- 5.2.2. Access changes should be submitted by email to the OMES Service Desk or by creating a CRM Case. All requests must include approval from the employee's management or DSR. The OMES Service Desk will then assign the case to the IS-Security Provisioning team.
 - 5.2.2.1. Management may need access to email or files in an employee's account to which they would normally not have access. Access will be granted for a supervisor to have access to an employee's account if the request is approved by the supervisor's management.
- 5.2.3. For network folder permission requests beyond the Onboarding case, a supervisor, manager or DSR must create a CRM Case. The CRM Case should include the desired network location.
- 5.2.4. The CRM Case is assigned to Security Provisioning to secure approval from the folder owner.
- 5.2.5. Accounts and access are disabled either at employee separations or when the account/access is no longer required to perform a job function.
 - 5.2.5.1. Upon employee separation, access is disabled as part of the Offboarding process (refer to **02.3.9 Offboarding**).
 - 5.2.5.2. Account disable requests must be acted upon at the time of receipt or the date indicated in the request.
 - 5.2.5.3. The Security Provisioning team runs a PowerShell script to remove access. The script disables the Active Directory account, removes the user from all permission groups, disables their email account, hides the user from the Global Address List and compresses their H drive. All of the user's Active Directory information is stored in text files on the file server.
 - 5.2.5.4. Data owners or the user's management may request to have an account or access disabled at any time, not just at employee separations.
- 5.2.6. User network account passwords expire every 60 days. The accounts will lock if the passwords are not changed. To have the account unlocked, the user must contact the OMES Service Desk for a password reset.
- 5.2.7. Accounts that go 60 days without use are disabled. Security Provisioning runs a monthly report to identify nonuse accounts. Users can request reactivation via CRM Case.

Number:	03.1.4	Page:	3 of 3
Latest Version:	1.1	Revision Date:	08/04/2016
Effective Date:	08/04/2016	Replaces:	1.0
Revised By:	Joshua Graves	Review Cycle/Date:	Annual
Reviewed By:	Laquetta Russell	Reviewing Unit:	Security Provisioning
Title:	Active Directory Identity Management SOP		
Description:	This document is the operating standard for Identity Management for Active Directory.		

6. Roles and Responsibilities

- 6.1. Chief Information Security Officer
 - 6.1.1. Reviews and authorizes use of generic user accounts.
- 6.2. System or Data Owners
 - 6.2.1. Reviews and authorizes use of generic user accounts.
- 6.3. Decentralized Security Representative
 - 6.3.1. Authorizes the restoration of deactivated user accounts.
 - 6.3.2. Approves access changes.
- 6.4. OMES Service Desk
 - 6.4.1. Creates Contractor IDs.
 - 6.4.2. Unlocks locked out accounts.
- 6.5. Security Provisioning
 - 6.5.1. Secures approval for network folder access.
 - 6.5.2. Creates, edits and disables user accounts.

7. References

- 7.1. 02.3.1 Onboarding
- 7.2. 02.3.9 Offboarding