

9400-S173: AD Privileged Access Standard

I. PURPOSE

This standard outlines general provisions for privileged access (see Policy 9400-P173: Logical Access Controls on Information Technology Resources) and enumerates general roles and responsibilities for the Enterprise, Schema and Domain Administrators roles within Active Directory (AD). The following applies to any Active Directory within the State

II. SCOPE

This standard applies to all executive branch agencies, boards, and commissions (collectively referred to as “agency” or “agencies”).

III. STANDARD

A. General

1. Privileged access shall only be granted upon completion or verification of background checks that meet or exceed the investigative requirements for the highest level of data the user will have access to.
2. UserIDs and passwords for privileged access shall be separate and distinct from user’s regular domain user accounts and shall not be used for non-privileged operations.
3. Contractors/vendors shall not be given privileged access to production systems unless negotiated as part of a Statement of Work (SOW) or maintenance agreement.
4. If privileged access is granted to complete a specific task, privileged access will be revoked once task is complete.
5. Privileged users shall comply with all State of Wyoming IT security policies, standards and statutes.

B. AD Enterprise Administrator Account

1. At least one permanent primary and one permanent secondary account shall be created.
2. Other than permanent accounts, assignment of Enterprise Administrator privileges will be driven by a specific task or function, and shall fall under the oversight of the agency’s Change Advisory Board (CAB).
3. Roles and Responsibilities:

9400-S173: AD Privileged Access Standard

- a. Maintain the AD at the forest level.
- b. Maintain the AD forest trusts.
- c. Maintain the integrity of the AD security boundary.
- d. Monitor and audit the activities of Domain Administrators.
- e. Perform only those tasks assigned and for which privileged access was granted.
- f. Maintain documentation in accordance with State or agency retention schedule.
- g. Cooperate and coordinate with the CAB for the orderly and expedient execution of change requests.

C. AD Schema Administrator account

1. Privileges will be assigned when a modification to the schema is needed.
2. Assignment of privileges will be performed by the Enterprise Administrator, and shall fall under the oversight of the agency's CAB.
3. Roles and responsibilities
 - a. Maintain the Active Directory schema.
 - b. Ensure the schema supports the integrity of the AD security boundary.
 - c. Perform only those tasks assigned and for which privileged access was granted.
 - d. Submit documentation of schema changes to the CAB.
 - e. Maintain documentation in accordance with State or agency retention schedule.
 - f. Cooperate and coordinate with the CAB for the orderly and expedient execution of change requests.

D. AD Domain Administrator account

1. At least one permanent primary and one permanent secondary account shall be created, and shall be monitored by the Enterprise Administrator.
2. Other than permanent accounts, assignment of Domain Administrator privileges will be driven by volume and urgency of daily operations or specific tasks and functions. Additional Domain Administrator accounts shall be monitored by the Enterprise Administrator.
3. Roles and responsibilities:
 - a. Maintain the day-to-day operation of domain trees that populate the forest.
 - b. Perform only those tasks assigned and for which privileged access was granted.
 - c. Submit completed non-routine and emergency change requests to the CAB.
 - d. Maintain documentation in accordance with State or agency retention schedule.

9400-S173: AD Privileged Access Standard

- e. Provide monitoring and reporting of anomalous activities.
- f. Maintain audit trails and event logs of security related activities.
- g. Provide on-site support during business hours and on call support after business hours.
- h. Supervise delegated administrative tasks to non-privileged users.

CIO Approved Date: 02/11/2010