UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Active Directory Policy
Policy #: Information Security-P#
Regulation: HIPAA, GLB, PCI DSS, State of Oklahoma
Effective: 09/10/03

Coverage: OUHSC
Version: 2.3
Approved: 09/10/03
Revised/Reviewed: 11/12/2014

Policy Summary: All information resources should be managed at an enterprise level utilizing Microsoft Active Directory.

Purpose: To help ensure the protection of University information resources and data by implementing the application of group security policies and configuration management.

Policy: All University owned or operated computers that are compatible with Microsoft Active Directory (AD) and connected to the University network must be a member of the University's enterprise domain.

As a member of the University's AD, all computers must be configured as follows:
- Computer must be named according to the appropriate naming scheme to aid in identification
- Computer must be placed in the appropriate Organizational Unit (OU) within the domain
- The "Managed by" field of the computers properties in AD needs to be populated with appropriate contact information
- The computer must have the appropriate "Domain Admins" group as a member of the local "Administrators" group

Documentation: All data collected and/or used as part of the Risk Management Process and related procedures must be formally documented and securely maintained by the Data Owner or a delegate.

Scope/Applicability: This policy is applicable to all OUHSC workforce members.

Regulatory Reference:
- HIPAA 45CFR Parts 160, 162, and 164.308(a)(1)(ii)(B), PCI DSS v3.0

Definitions: See the Information Security Policy Definitions document for definitions

Responsible Department: Each OUHSC business unit within the OUHSC that manages information system resources is responsible for complying with this policy.

Enforcement/Audit: The University's Internal Auditing department is responsible for monitoring and enforcing this policy.

Related Policies: in support of the Antivirus and Risk Management Policies

Renewal/Review: This policy is to be reviewed and updated as needed by IT Information Security Services.