Active Directory Authentication Policy

Purpose
The purpose of this policy is to specify the appropriate method for authenticating with the Auburn domain Active Directory.

Policy
Any application that uses the Auburn domain Active Directory for authentication must use a secure method of authentication to minimize exposure of user passwords.

Applications found to be operating in a non-secure mode will be shut down.

Implementation Guidelines
Application designers who are designing applications that require Lightweight Directory Access Protocol (LDAP) authentication with the Auburn domain Active Directory are encouraged to contact the appropriate unit IT provider or OIT for assistance. A list of IT providers is available online at: http://www.auburn.edu/oit/it_directory.php

Applications that use simple LDAP binds or other un-secure methods of authentication to Auburn’s Active Directory LDAP are not allowed.

Scripts used to maintain Active Directory Groups or otherwise manage an Organizational Unit (OU) must use secure forms of authentication.

Currently approved secure authentication methods include secure LDAP, Kerberos, or Windows NT LAN Manager (NTLM). However, other methods may become available in the future.

Issued by: The Office of the Executive Director, OIT

ADOPTED: December 08, 2005