UW-Madison
Access Control Services Policy

Policy
All UW-Madison units that maintain or operate electronic services secured by access controls must configure those applications or systems to:

1. use institutionally managed access control services as suitable services become available,
2. comply with the appropriate use standards for the institutionally managed credentials.

Background
In August of 2006 the NetID Policy Issues Team and the AuthN/Z Coordinating Team, composed of representatives from a variety UW-Madison units, made policy recommendations for the use of institutionally managed credentials and institutionally managed access control services. The recommendations were reviewed by the CIO and endorsed by the Identity Management Leadership Group. The recommendations seek to:

1. improve security by:
   a. reducing the number of electronic services that store credentials and
   b. establishing more uniformity among services that store credentials,
2. reduce confusion by clearly distinguishing institutionally managed credentials from locally managed credentials,
3. better enable the use of “single sign-on”, reducing the number of credentials needed, and
4. facilitate wider access by:
   a. increasing the populations supported by the institutional access control services and
   b. improving support for federated access control to or from external applications.

Authority
Issued by the UW-Madison Vice-Provost for Information Technology.

Enforcement
1. Designated representatives of the UW-Madison CIO and Vice-Provost for Information Technology will set the current compliance standard and determine whether or not an application or system is in compliance.
2. The standard for compliance is expected to change over time as suitable access control services become available and barriers to migration are reduced.

Contact
Please address questions or comments to policy@cio.wisc.edu.

References
Access Control Services Standard: https://kb.wisc.edu/itpolicy/cio-access-control-services-standard
IT Policy Glossary: https://kb.wisc.edu/itpolicy/glossary
UW-Madison

Access Control Services Standard

These standards for compliance are for the Access Control Services Policy.

1. Policy provision 1 requires that electronic services secured by access controls be configured to use institutionally managed access control services as suitable services become available. Current institutional managed access control services include:

   a. NetID Login Service
      To begin using this service, please see the NetID Login Service description (https://it.wisc.edu/services/netid-login-service/), or search the DoIT Help Desk Knowledge Base (http://kb.wisc.edu/search.php?q=netid+login+service.)

   b. Campus Active Directory
      To begin using this service, please see the Campus Active Directory description (https://it.wisc.edu/services/campus-active-directory/), or search the DoIT Help Desk Knowledge Base (http://kb.wisc.edu/search.php?q=active+directory+service.)

Special Cases:

If the NetID Login Service cannot meet the needs of an application or system, and it is still desired that the application or system authenticate using NetID, special NetID authentication arrangements can be made under the following conditions:

   a. A UW-Madison unit must request that an application or system be authorized to use NetID by submitting the “Identity Data Integration Request” form at http://it.wisc.edu/services/iam

   b. For an application or system to handle NetID and password, the following steps need to be taken:
      1) Appropriate security controls must be in place to protect NetID and password, for example, encryption of the password.
      2) There must be an initial and periodic audit to assure that the appropriate security controls are adequately implemented and operational.
      3) Staff who develop or manage the authenticating application or system must be trained to use and maintain NetID authentication in a secure manner.

   c. Specific applications, systems or agreed upon deployment limits must be identified that can meet the requirements above.

Exceptions:

UW-Madison applications and systems are exempt if migration to the available institutionally managed access control services is currently impractical for technical or operational reasons.

   a. Example technical reason: the available institutionally managed access control services do not support an access control method compatible with the system or application.

   b. Example operational reason: the migration of several different systems or applications must be coordinated because they share a locally managed credential.

The number of applications and systems that qualify for an exemption will become smaller as the capabilities of the institutionally managed access control services are expanded to support a wider range of applications and systems.
2. Policy provision 2 requires that electronic services secured by access controls be configured to comply with the appropriate use standards for the institutionally managed credentials. Current appropriate use standards include:
   
a. NetID Appropriate Use Standards
   
b. University Directory Service (UDS) Responsible Use Policy

Additional appropriate use standards may be adopted as institutionally managed credentials are added.