

# UW-Madison Policy for Use of Institutional Access Control Services

## 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<sup>1</sup>, 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<sup>2</sup> were reviewed by the CIO and endorsed by the Identity Management Leadership Group<sup>3</sup>. The recommendations seek to:

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

## Authority

This policy is issued by the UW-Madison CIO and Vice-Provost for Information Technology.

## Compliance

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

## Related Documents

The glossary and attached compliance standards are an extension of the policy.

See: <https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary>

## Contact

Please direct questions about this policy to [policy@cio.wisc.edu](mailto:policy@cio.wisc.edu).

---

<sup>1</sup> Information about NetID PIT and ACT is at: <https://wiki.doit.wisc.edu/confluence/display/AUTHNZ/Home>.

<sup>2</sup> The NetID PIT report may be viewed at: <https://wiki.doit.wisc.edu/confluence/display/POLICY/NetID+PIT>.

<sup>3</sup> The IMLG web site is at: <http://registrar.wisc.edu/imlg/>.

Policy ID: IAccess      Maintained by: Office of the CIO, Policy and Planning Department  
Effective: Dec 1, 2009      Revision: October 20, 2009 (review period: two years)

# Compliance Standards

## UW-Madison Policy for Use of Institutional Access Control Services

These compliance standards are for the UW-Madison Policy for Use of Institutional Access Control Services. Please see the [glossary](https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary) at <https://wiki.doit.wisc.edu/confluence/display/POLICY/Glossary>. For further background see: <https://wiki.doit.wisc.edu/confluence/display/POLICY/IAccess>.

### **A. Current Compliance Standards:**

1. Regarding the requirement that electronic services secured by access controls be configured to use institutionally managed access control services as suitable services become available:

#### **Available Access Control Services:**

Additional capability may be added to existing access controls services, or other access control services may be added. Current access control services include:

- (a) NetID Login Service. To begin using this service, please see: <http://login.wisc.edu/docs>.
- (b) Campus Active Directory. To begin using this service, please see: [http://www.doit.wisc.edu/middleware/active\\_request.asp](http://www.doit.wisc.edu/middleware/active_request.asp)

#### **Exceptions:**

It is anticipated that the number of applications and systems that qualify for an exemption will become smaller as the barriers to migration are reduced, and the capabilities of the available access control services are expanded to support a wider range of applications and systems.

Current exceptions include:

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

Example technical reasons: the available access control services do not support an access control method compatible with the system or application.

Example operational reasons: some consumer populations cannot yet obtain a NetID, or the migration of several different systems or applications must be coordinated because they share a locally managed credential.

2. Regarding the requirement 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:**

Over time, additional appropriate use standards may be adopted when more institutionally managed credentials are added. Current appropriate use standards include:

- (a) Appropriate Use Standards for NetID,  
See: <https://wiki.doit.wisc.edu/confluence/display/POLICY/NetID+AUS>.
- (b) Appropriate Use of University Directory Service (UDS) Data Policy  
See: <http://www.doit.wisc.edu/middleware/uds/use.asp>.

#### **Exceptions:**

The individual appropriate use standards address exceptions to the standard.

Policy ID: IAccess      Maintained by: Office of the CIO, Policy and Planning Department  
Effective: Dec 1, 2009      Revision: Oct 29, 2009 (review period: one year or sooner as needed)