Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Identity and Access Management Standard for State Government Agencies

Category	**Security Architecture**
Title	**Identity and Access Management Standard for State Government Agencies.**
Number	

Applicability

☑ **State Government Agencies, excluding** Higher Education; and agencies receiving an exemption pursuant to Section 4.2……..... **Standard**
☐ **State Government Agencies,** all .....**Not Applicable**
☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**
☐ **Other: _____** .....**Not Applicable**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document.
Guideline - Adherence is voluntary.

Status	☑ Adopted ☐ Draft ☐ Other:_____
Dates	Date: March 15, 2005 Date Adopted by NITC: March 15, 2005 Other: To be reviewed annually by the Technical Panel.

Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard:

All state government web applications that require authentication and authorization of users will utilize the enterprise directory, known as Nebraska Directory Services.

2.0 Purpose and Objectives:

The purpose of this standard is to provide an enterprise solution for identity and access management capabilities to reduce security administration costs, ensure regulatory compliance, and increase operation efficiency and effectiveness. This standard focuses on web applications, because most if not all new applications will utilize web technology. To incorporate non-web applications into the Nebraska Directory Services would require additional cost and different policies to implement.

Objectives include:

- Build an identity-based portal that can integrate disparate applications, enable secure web access to applications and data, and enable users to access applications from their offices or remote locations.
- Implement a standardized, secure identify and access management architecture that provides centralized management with local administration of users, centralized user identity information, synchronized user identity information across multiple applications (where appropriate), and application-level authentication and authorization based on the unique identity of the user (as opposed to a shared logon ID).
- Use standards-based technology to ease application integration, provide for reuse of components and remain adaptable in the face of changing technology products.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for identity and access management, including HIPAA and NCIC security regulations.
- Provide a high level of security including the option of two-factor identification.

3.0 Definitions:

3.1 Authentication – The process of uniquely identifying an individual. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

3.2 Authorization – The process of giving individuals access to system objects based on their identity which allows them to add, update, delete or view information for a web application.

3.3 Identify and Access Management – Enterprise Identity Management is a system of technologies, business practices, laws and policies that manages common identification of user objects; reduce the costs while enhancing the quality of government services; protects the integrity of state resources; and safeguards the privacy of the individual.

3.4 LDAP – LDAP (Lightweight Directory Access Protocol) is an Internet protocol that applications use to look up user information from a server, such as Novell's eDirectory.

3.5 Web Applications – Web server based applications that are accessed using a web browser. This definition includes custom developed systems and third party software systems.

4.0 Applicability

4.1 State Government Agencies

This standard applies to all state government agencies, boards, and commissions, except Higher Education and those agencies receiving an exemption under Section 4.2.

4.1.1 State Agencies, Boards, and Commissions

All new web applications requiring authentication and authorization of individuals must comply with the standard listed in Section 1.0. All existing web applications requiring authentication and authorization must convert to the standard listed in Section 1.0 as soon as fiscally prudent or upon an upgrade to the web application, whichever comes first, unless the application is exempt.

4.2 Exemption

Exemptions may be granted by the Technical Panel of the NITC upon request by an agency.

4.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the Technical Panel of the NITC. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the CIO via e-mail or letter (Office of the CIO, 521 S 14th Street, Suite 301, Lincoln, NE 68508). The Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 IMServices

IMServices will incorporate the needed hardware and software into their infrastructure to provide the following:

- LDAP directory for user /entity objects.
- Role-based authentication and authorization to the enterprise LDAP directory and applicable applications for registered users.
- Business/disaster recovery.
- Authentication methods available:
  - User ID and password
  - Two-factor authentication
  - X.509 certificates

5.2 State Agencies, Boards and Commissions

Agencies, Boards and Commissions will carry out the following responsibilities:

- Web applications requiring authentication and authorization must comply with the standard listed in Section 1.0.
- Require this standard be referenced in all RFPs (Requests for Purchase) for web applications covered by this standard.

5.3 State Government Council Directory Services Workgroup

The State Government Council's Directory Services Workgroup will provide ongoing advice and direction, including but not limited to:

- Policies for implementation;
- Benchmarks and service level agreements;
- Funding options.

6.0 Related Policies, Standards and Guidelines

- NITC Information Security Management Policy – January 23, 2001
- NITC Access Control Policy – January 23, 2001
- NITC Network Security Policy – January 23, 2001
- State Government Council's Directory Services Workgroup Phase I recommendation – July 30, 2003