

Technical Panel
of the
Nebraska Information Technology Commission

Standards and Guidelines

**Draft Document
30-Day Comment Period**

Title: Password Standard

[NOTE (August 10, 2007): The posting of this document for the 30-day comment period is subject to the approval of the Technical Panel at their meeting on August 14, 2007. At that time, the Technical Panel may approve the posting of this document, or the Technical Panel may choose to withdraw this document from the comment period.]

Notes to Readers:

1. The following document is a draft document under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at <http://nitc.ne.gov/standards/>.
2. If you have comments on this document, you can send them by email to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on September 9, 2007.
4. The Technical Panel will consider this document and any comments received at their next meeting following the comment period, currently scheduled for September 11, 2007. Information about this meeting will be posted on the NITC web site at <http://nitc.ne.gov/>.



Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Password Standard

Category	Security Architecture
Title	Password Standard
Number	

Applicability	<input checked="" type="checkbox"/> State Government Agencies <input type="checkbox"/> All..... Not Applicable <input checked="" type="checkbox"/> Excluding higher education institutions Standard <input type="checkbox"/> State Funded Entities - All entities receiving state funding for matters covered by this document..... Not Applicable <input checked="" type="checkbox"/> Other: All Public Entities Guideline Definitions: Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.2). Guideline - Adherence is voluntary.
---------------	--

Status	<input type="checkbox"/> Adopted <input type="checkbox"/> Draft <input type="checkbox"/> Other: _____
Dates	Date: Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
 Authority: Neb. Rev. Stat. § 86-516(6)
<http://www.nitc.state.ne.us/standards/>

1.0 Standard

Passwords are a primary means to control access to systems; therefore all users must select, use, and manage passwords to protect against unauthorized discovery or usage.

1.1 Password Construction

The following are the minimum password requirements for State of Nebraska passwords:

- Must contain at least eight (8) characters
- Must contain at least three (3) of the following four (4):
 - At least one (1) uppercase character
 - At least one (1) lowercase character
 - At least one (1) numeric character
 - At least one (1) symbol
- Must change at least every 90 days
- Must not repeat any character sequentially more than two (2) times
- Can not repeat any of the passwords used during the previous 365 days.

1.2 Non-Expiring Passwords

Agencies may use non-expiring passwords for automated system accounts (e.g. backups and batch jobs) after submitting the form found in Appendix A. All non-expiring passwords should exceed the character requirements listed in Section 1.1.

2.0 Purpose and Objectives

Passwords are used to authenticate a unique User ID to a variety of State of Nebraska resources. Some of the more common uses include: user accounts, web accounts, email accounts.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption

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

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; system limitation, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 501 S 14th Street, Lincoln, NE 68509). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State Agencies

Each state agency will be responsible for ensuring that any application or system requiring the use of a password adheres to this standard.

5.0 Related Documents

5.1 NITC Information Security Policy (<http://www.nitc.state.ne.us/standards/index.html>)

5.2 Non-expiring Password Agreement (Appendix A)

Appendix A

Non-Expiring Password Agreement

This agreement describes the agreed upon policy exception and/or level of security provided by the Office of the CIO for the application known as:

To the limits dictated by the State of Nebraska and Federal laws, agency data and system owners are responsible for determining how critical and sensitive information is for their applications to insure integrity, availability, and confidentiality.

Security Classification Levels

The NITC Data Security Standard recognizes four basic levels of security classifications that are associated with varying degrees of known risks. (See NITC Security Officer Handbook for more details). They can be summarized as follows:

HIGHLY RESTRICTED is for the most sensitive information intended strictly for use within your organization and controlled by special rules to specific personnel. It is highly critical and demands the highest possible security.

CONFIDENTIAL is for less sensitive information intended for use within your organization, yet still requires a high level of security. It may be regulated for privacy considerations. (e.g. HIPAA)

INTERNAL USE ONLY is for non-sensitive information intended for use within your organization. The security is controlled, but not highly protected.

UNCLASSIFIED/ PUBLIC is for information that requires minimal security and can be handled in the public domain.

Agency Justification

The undersigned agency representative has been authorized to request a **non-expiring password** for the application and data named above with a **security classification level** of _____ and includes the following criteria as supporting justification:

* * * * *

Office of the CIO Justification

The Office of the CIO recommends **no policy exceptions** with the following justification:

Agency Representative

Date

Office of the CIO Representative

Date