NITC 8-301

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 8-301

Title	Password Standard
Category	Security Architecture
Applicability	Applies to all state agencies, boards, and commissions, excluding higher education

1. Purpose

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.

2. Standard

2.1 Password Construction

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

- Must contain at least eight (8) characters
    - Must not repeat any character sequentially more than two (2) times
- 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
- Can not repeat any of the passwords used during the previous 365 days.

2.2 Non-Expiring Passwords

An agency may request a non-expiring password by submitting the form found in Appendix A. All non-expiring passwords should meet the character requirements listed in Section 2.1.

2.2.1 Automated System Accounts. Agencies may use non-expiring passwords for automated system accounts. Examples of automated system accounts include those that perform backups or run batch jobs.

2.2.2 Multi-user Computers. Agencies may use non-expiring passwords on multi-user computers. Examples of multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources.

2.2.3 System Equipment/Devices. It is common for many devices (e.g. IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID and password in a manner similar to those found while authenticating a user, the distinction to be made is that the User ID is used to authenticate the device itself to the system and not a person.

Attachment A: Non-Expiring Password Request (Word Document)

HISTORY: Adopted on September 18, 2007. Amended on November 12, 2008.
PDF FORMAT: http://nitc.ne.gov/standards/8-301.pdf

NITC 8-301
Attachment A

Non-Expiring Password Request

This is a request for a non-expiring password for the following application, system, or account:

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 8-RD-01: NITC Security Officer Instruction Guide). 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 as supporting justification:

____

____

* * * * *

Office of the CIO Action

___ Granted   ___ Denied

Comments:

_______________________________	___________	_______________________________	____________
Agency Representative	Date	Office of the CIO State Information Security Officer	Date