NITC 8-301.01

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 8-301.01 (Draft)

Title	Password and Authentication Standard for Public Applications
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 applications. The purpose of this standard is to require all users to create, use, and manage passwords to protect against unauthorized discovery or usage.

2. Standard

For Public Applications, the following standards require a minimum level of password complexity and define the application's handling of invalid login attempts, password reset and notification requirements.

2.1 Access Requirements

One of the following methods of access will be utilized:

2.1.1 Password Access

The following are the minimum public password construction requirements:

- Must contain at least eight (8) characters
- Must contain at least three (3) of the following four (4) requirements:
  - At least one (1) uppercase character
  - At least one (1) lowercase character
  - At least one (1) numeric character
  - At least one (1) symbol

2.1.2 PIN Access

The following are the minimum PIN access requirements:

- Must contain at least 4 digits/characters.
- PIN must be pre-generated and given to user through a separate process such as email.

2.2 Password Expiration

Passwords will expire at least every 14 months. The user cannot re-use any of the last three (3) passwords used. Passwords will have a minimum time between user initiated resets of one (1) day.

2.3 Account Lock-out

The following are the minimum lock-out required procedures:

- Accounts not used within 14 months will be marked as inactive.
- Accounts not used within 24 months must be removed from the system.
- Three (3) consecutive failures to enter a correct password will lock-out the account for a minimum of 3 minutes.
- If the user provided an email address while setting up the account, they must be notified by email when the account has been locked-out.

2.4 Account Re-activation

One of the following methods must be utilized when re-activating a user's account:

- Must successfully answer 2 of the 3 security questions presented.
- Identity must be verified by a successful response to an email validation request.

2.5 Data Security Requirements

Access to information must comply with all local, state and federal safeguard requirements. Access to information must comply with any Agency specific information policy. All data must be classified using the classification safeguard requirements.

[NITC 1-101: Definitions]

Add the following new definitions to NITC 1-101: Definitions.

Personal Identification Number (PIN): The multiple digit access code generally used in securing systems having only numeric entry ability. Can also used as form of information utilized for identifying account access.

Public Application: Software that is primarily utilized by citizens and State business partners.

DATE: Draft - July 8, 2013
HISTORY:
