State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

AMENDMENTS TO NITC 8-301

1. Strike the original sections and insert the following new sections:

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

1. Purpose

The purpose of this standard is to set the minimum requirements for passwords and the related system access requirements based on the data classification (NITC 8-101, § 4.6).

1.1 Scope

The scope of this standard is restricted to passwords that are used to authenticate users to networks or applications.

1.2 Minimum Password Complexity Construction

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

- Must contain a minimum 8 characters
- Must contain at least three (3) of the following four (4) :
    - At least one (1) upper case character
    - At least one (1) lowercase character
    - At least one (1) numeric character
    - At least one (1) symbol
- Cannot repeat any of the passwords used during the previous 365 days.

2. Standard

In addition to the Minimum Password Complexity outlined in section 1.2, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All employees and contractors of the State of Nebraska shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

2.1 Highly Restricted

Information that is deemed highly restricted requires the highest level of security. A password used to access Highly Restricted information must follow the password

complexity rules outlined in section 1.2 and must contain at least 2 of the following additional requirements:

- Multi Factor Authentication
- Expire after 60 days
- Minimum Password Age set to 15 days

2.2 Confidential

Information that is deemed Confidential requires a high level of security. A password used to access Confidential information must follow the password complexity rules outlined in section 1.2 and must contain the following additional requirement:

- Expire after 90 days

2.3 Managed Access Public

Information that is deemed Managed Access Public requires minimal level of security and need not comply with section 1.2 of this policy. Typically this data would not include personal information but may carry special regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service to users that have subscribed to a service.

2.4 Public

Information that is deemed Public requires no security and need not comply with section 1.2 of this policy. This information should be restricted to view only.

3.0 Non Expiring Passwords

Non Expiring Passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in section 1.2. The additional requirements for access to confidential data with a non-expiring password are:

- Must contain at least one of the following additional security features:
    - Extended password length to 10 characters
    - Personal security question may be asked
    - Multi Factor Authentication
    - Any feature not included on this list may also be utilized upon approval of the State Information Security Officer or upon enactment of federal, state or departmental laws, policies or directives.

3.1 Automated System Accounts

Agencies may use non-expiring passwords for automated system accounts. Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs.

3.2 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.

3.3 System Equipment/Devices

Agencies may use non-expiring passwords for 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.