8-302. Passwords.

(1) Minimum Password Requirements. The following are the minimum password requirements for state government passwords:

(a) Must contain a minimum of eight characters;

(b) Must contain at least three of the following four: at least one uppercase character; at least one lowercase character; at least one numeric character; or, at least one symbol (!@#$%^&); and

(c) Cannot repeat any of the passwords used during the previous 365 days.

In addition to the minimum password complexity outlined above, 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 shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

(2) Additional Access Requirements for RESTRICTED Information. Information that is classified as RESTRICTED requires the highest level of security. This includes root/admin level system information accessed by privileged accounts. A password used to access RESTRICTED information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:

(a) Multi-factor authentication;

(b) Expire after 60 days;

(c) Minimum password age set to 15 days; and

(d) Accounts will automatically be disabled after three unsuccessful password attempts.

(3) Additional Access Requirements for CONFIDENTIAL Information. Information that is classified as CONFIDENTIAL requires a high level of security. A password used to access CONFIDENTIAL information must follow the password complexity rules outlined in subsection (1), and must contain the following additional requirements:

(a) Expire after 90 days; and

(b) Accounts will automatically lock after three consecutive unsuccessful password attempts.

(4) Password Requirements for MANAGED ACCESS PUBLIC Information. Information that is classified as MANAGED ACCESS PUBLIC requires minimal level of security and need

not comply with subsection (1). 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.

(5) Password Requirements for Accessing PUBLIC Information. Information that is classified as PUBLIC requires no additional password security and need not comply with subsection (1).

(6) 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 subsection (1). The additional requirements for access to CONFIDENTIAL or RESTICTED data with a non-expiring password are:

(a) Extended password length to 10 characters;

(b) Independent remote identity proofing may be required;

(c) Personal security question may be asked;

(d) Multi-factor authentication; and

(e) Any feature not included on this list may also be utilized upon approval of the state information security officer.

(7) 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. System account passwords shall expire after 365 days, unless mechanisms to restrict the use of those credentials to just the authorized service can be implemented and approval is granted by the state information security officer.

(8) Multi-User Computers. Multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources. Agencies may use non-expiring passwords on multi-user computers. In these cases, mechanisms to ensure the user account with non-expiring passwords is unable to access CONFIDENTIAL or RESTRICTED information.

(9) 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 like 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.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-302.pdf