

**DOUGLAS COUNTY ADMINISTRATIVE
POLICIES AND PROCEDURES**

NUMBER: 100.34
EFFECTIVE DATE: 1/07/16
LAST REVIEWED: 5/19/22
LAST REVISED: 5/19/22
AUTHORITY: BOCC
COUNTY MANAGER: 
PAGE 1 OF 3

SUBJECT: PASSWORD POLICY

- I. PURPOSE:** Douglas County recognizes that strong passwords are one layer of a multi-faceted approach to providing good network security and protecting the data that resides on the County network. This policy provides guidance and requirements for the creation and maintenance of passwords that all personnel must adhere to when accessing any County network resources.
- II. POLICY AND PROCEDURES:**
- A. AUTHORITY TO ACCESS COUNTY NETWORK:**
1. All County employees and authorized users that require access to any network, system, or application that resides on or is controlled by Douglas County Technology Services (DCTS) must satisfy a user authentication mechanism such as a unique user identification (User ID) and password, a biometric input, or a user identification smart card to verify their identity.
 2. Anyone seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, or other authentication information.
 3. Generic accounts are not authorized. Each user must use their individually assigned account at all times when accessing the County network.
- B. UNIQUE USER IDENTIFICATION:**
1. Any employee or authorized user who requires access to any network, system, or application controlled by DCTS must have completed an appropriate background check through Douglas County Human Resources prior to being granted access. Outside agencies and/or vendors/contractors that have been vetted by other means will be accepted upon verification and approval by Douglas County Human Resources.
 2. If an employee or authorized user believes their User ID has been compromised, they must report that incident to DCTS immediately.

- C. SECURITY PASSWORD MANAGEMENT:
1. All employees and authorized users must create a password in conjunction with their User ID to gain access to any network, system, or application. This password must be kept confidential and must not be shared with anyone.
 2. A password used to access a County network, system, or application must not be used for any other application or account that requires a password or other authentication, whether for County business or personal use.
 3. All passwords used to access any network system or application must meet the following standards:
 - a) Passwords must be a minimum of 10 characters in length.
 - b) Passwords must incorporate a minimum complexity that includes the following characteristics:
 - i. At least one lower case letter (a-z)
 - ii. At least one upper case letter (A-Z)
 - iii. At least one number (0-9)
 - iv. At least one punctuation or non-alphanumeric characters found on a standard ASCII keyboard (e.g. ! @ # \$ % ^ & * () _ - + = { } [] ; : “ ’ \ / ? < > , . ~ `).
 - c) Passwords should not contain any words found in a dictionary or that can be easily guessed.
 - i. Some examples of passwords to avoid are: “The Giants are #1,” “I own 6% of my house,” “I am 2 degrees from Kevin Bacon!”
 - ii. Examples of better passwords: “DaB3ar’s<3,” “7heS3Rmycreds!,” “@W0rk!l0lz&l0lz,” and “T1c/t4ct0w.”
 4. Passwords will expire after 90 days and the previous five passwords used will be remembered and cannot be reused.
 5. An account lock-out will occur if an individual attempts to login with incorrect credentials five times within a 30 minute period. The lock-out will reset automatically after 30 minutes, after which the user may make another attempt to log in.
 6. Every user is responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
 - a) Passwords are only to be used for legitimate access to networks, systems, or applications.
 - b) Passwords must not be disclosed to other staff members or individuals.
 - c) Each account must only be accessed by the user assigned to the account. Acceptable exceptions to this are when working with DCTS or a vendor to troubleshoot any errors. If DCTS requires a user’s password to troubleshoot any error, DCTS will reset the user’s password and the user must change their password after the problem is resolved. If a vendor obtains a user’s password for any reason, the user must immediately change their password.

- d) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on/near the workstation. Passwords must not be saved in any files or emails on the network unless encrypted by an authorized password management program. The password feature in Microsoft Office programs is not sufficiently secure and may not be used to protect County network or application passwords.

III. RESPONSIBILITY FOR REVIEW: The Internal Review Committee shall review this policy as needed or at least once every 3 years.