8-304. Privileged access accounts.

Privileged access accounts include administrator accounts, embedded accounts used by one system to connect to another, and accounts used to run service programs. These accounts are used by systems and personnel to access sensitive files, execute software, load and configure policies and configuration settings, and set up or maintain accounts.

Due to the elevated access levels these accounts typically have, the following standards and procedures must be followed to minimize the risk of incidents caused by these accounts:

(1) All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts must not be shared;

(2) All privileged access accounts must use OCIO-approved multi-factor authentication where technically possible;

(3) Service accounts must not be used to interactively log in to a system or resource;

(4) Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed;

(5) Default system account credentials for hardware and software must be either disabled, or the password must be changed. Use of anonymous accounts is prohibited, and unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account must be disabled. At all times, the state requires individual accountability for use of privileged access accounts;

(6) Privileged access accounts must have enhanced activity logging enabled and reviewed at least quarterly;

(7) Privileged access through remote channels will be allowed for authorized purposes only and must include multi-factor authentication;

(8) Passwords for these accounts must be changed every 60 days;

(9) The password change process must support recovery of managed systems from backup media. Historical passwords should remain accessible in a history table in the event that they are needed to activate a backup copy of a system; and

(10) Privileged access accounts must be approved, provisioned, and maintained by the Office of the CIO.

Exceptions to this policy may be granted by the state information security officer.

--

History: Adopted on July 12, 2017. Amended on March 10, 2022 and November 10, 2022.
URL: https://nitc.nebraska.gov/standards/8-304.pdf