



LAN Password Procedures

The System Administration LAN password standards, below, were developed based on information from a number of sources, including: New York State Cyber Security policy, common best practices, management advice, and System Administration software characteristics (i.e. password construction limitations etc.).

An initial common password is set for new users, which the new user must change immediately upon first login.

Standards for LAN Passwords

Passwords cannot resemble the person's User Id

Maximum password lifetime:	90 days	
Minimum password lifetime:	14 days	See details below
Minimum password length:	8	Characters/numbers
Password remembered history:	5	See details below
Password complexity enforced:	Yes	See details below
Number of failed attempts prior to lockout	6	See details below
Duration of lockout	1 hour	

Users are notified of impending LAN password expiration upon each logon, beginning at 14 days prior to expiration date, and offered the opportunity to change the password at that moment. This warning/notification gives users time to create and memorize a new password.

Password remembered history

A password cannot be reused until at least five (5) other passwords have been used. If a password is kept for the full 90-day duration, a password re-use (if desired by the user) could only occur after 18 months. Re-using passwords is not recommended, nor is using a predictable series of passwords with minimal changes that could be guessed if the previous password is known.

Minimum password lifetime

Users may elect to change passwords at any time after 14 days since the last change. The minimum password lifetime prevents users from circumventing the requirement to change passwords by doing five password changes in a minute to return to the currently expiring password.

Password resets can also be done by request with the Helpdesk or LAN services. Requests must come from the user or from an appropriate supervisor with adequate explanation, or by authorized request from legal or personnel sources and approved by the CTO.



Password complexity enforced

Password complexity requires that the password contain characters from three of the following four categories:

- Uppercase alphabet characters (A–Z)
- Lowercase alphabet characters (a–z)
- Arabic numerals (0–9)
- 32 Non-alphanumeric characters (for example, !\$,#,%)

Examples of complex passwords:

- D5a1v5e59 - combining First name and Date of Birth
- 5UNY\$ystem - use of numbers “5” or characters “\$” to replace letters “S”
- AtDhVaAnNkCsE! - use of a phrase to remember, such as “Thanks in ADVANCE!”
- Thanks in advance! - even that works, as long as a non-alpha (!) is in there.

The Online Microsoft password checker is a good source to check password concepts. It dynamically provides feedback on password construction and ranks passwords: WEAK MEDIUM STRONG BEST.

http://www.microsoft.com/athome/security/privacy/password_checker.msp

It also gives advice, “Strong passwords: How to create and use them.”

<http://www.microsoft.com/athome/security/privacy/password.msp>

Number of failed attempts prior to lockout

A user can attempt to sign-on six (6) times using incorrect information before the User ID is locked-out or prevented from attempting to again. The duration of lock-out is one (1) hour.