

Password Policy

All staff user accounts are to be subject to the password policy stipulated below:

- 1) Number of day(s) after which a password must be changed: 180
- 2) Number of day(s) before a password may be changed: 1
- 3) Minimum number of characters in a password: 8
- 4) Number of old passwords that cannot be re-used: 14
- 5) Complexity Requirements:

a) Passwords must not contain the staff members name (or parts of it):

- i. The username is checked in its entirety only to determine whether it is part of the password.
- ii. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters. The display name is broken into tokens, delimited by commas, periods, dashes or hyphens, underscores, spaces. Tokens that are less than three characters in length are ignored, and substrings of the tokens are not checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin," "M," and "Hagens." Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.

b) Passwords must contain characters from three of the following four categories:

- i. Uppercase (A through Z)
- ii. Lowercase (a through z)
- iii. Digits (0 through 9)
- iv. Non-alphanumeric characters: ~!@#\$%^&* -+=`|\(){}[]:;'"<>.,?/

Adopted: March 25, 2014; Amended: May 18, 2017; Reviewed: June 2021