



Information Services Department Computer Security Password Policy

Purpose: The purpose of this policy is to ensure that all CU Medicine employees are aware of and will adhere to strong and secure password policies.

Scope: The following guidelines apply to all computer passwords for all CU Medicine employees.

Policy: Strong and secure passwords have the following characteristics:

- Password length. Longer passwords are more difficult to break and should be at least 8 characters long.
- Expiration. Passwords expire within 45 – 60 days on CU Medicine computer systems.
- Dictionary checks. Strong passwords do not use regular words.
- Name prohibitions. Strong passwords do not include user names, names of relatives or pets, etc.
- Complexity. Include uppercase, lowercase, numeric and special characters.
- Good password examples:
 - s2neF(ceMtn (stone face mountain)
 - 10v1nghUSb#nd (loving husband)
 - fr0Zen&cre^my (frozen and creamy)
 - 41ceCre\$m (for ice cream)
- Re-use. It is best not to reuse passwords.
- Lockout. After five failed login attempts, accounts on CU Medicine computer systems will be locked out and must be re-enabled by the CU Medicine HelpDesk.