Cottonwood, Inc.
Policies and Procedures

SECTION: Information Technology **POLICY NO:** 07-003

SUBJECT: Account Passwords

EFFECTIVE DATE: April 2023

Policy:

Passwords are needed as a defense against unauthorized access to your account. Strong passwords can reduce the risk of cybercriminals guessing your password and accessing your computer or data.

Procedures:

Strong passwords can help defend against cyberattacks and lower the risk of a security breach. The following guidelines should be followed to create strong passwords:

- Use nine or more characters.
- Must contain characters from three of the four classes of characters.
  - English uppercase letters (A, B, C).
  - English lowercase letters (a, b, c).
  - Arabic numerals (1, 2, 3).
  - Special characters (!, *, $, or other punctuation symbols).
- Can't contain any part of a user's full name or username.
- Don't use any term that could easily be guessed by someone who is familiar with you.
- Don't include any personal information, e.g., the name of a spouse or a street address.
- Should not contain personal identification numbers, including those on a license plate, your telephone number, birth date, or any part of your Social Security number.

Don't keep a copy of your password in a desk drawer, on a monitor, or under a keyboard.

If you do keep a copy, put it in your wallet or purse.

Protect your password. Your password is yours alone.

Don't share it with anyone, including supervisors, personal assistants, or co-workers. In the event the IT Department needs your password you should change it immediately after the issue has been resolved.

Do NOT:

- Say your password aloud.
- E-mail your password to a co-worker.
- Offer anyone hints about what your password might be.

Passwords must be changed at least every 90 days.