Revised: 06/2022

Cottonwood, Inc.
Policies and Procedures

SECTION: General **POLICY NO:** 02-024

SUBJECT: Computer Internet and E-Mail use

EFFECTIVE DATE: April 1999

Policy:

It is Cottonwood, Inc.'s intent that the Internet and E-mail be used in a professional, secure and prudent manner.

Procedures:

1. E-Mail and Internet Usage
    a. It is permissible to use the company mail system and Internet Access for incidental personal purposes. This does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate company policy with regard to employee time commitments or company equipment.
    b. Employees may not use company E-Mail, Internet, or electronic messaging systems to infringe the copyright or other intellectual property rights of third parties, to distribute defamatory, fraudulent or harassing messages, or otherwise to engage in any illegal or wrongful conduct.
    c. Employees may not use company E-Mail, the Internet, or electronic messaging systems to download software unless they comply with established policies to check all such software for computer viruses.
    d. The unauthorized use of electronic messaging systems for purposes of "snooping" is a violation of company policy and will be grounds for dismissal.
2. E-Mail Content
    a. Employees may only forward E-Mail that has a legitimate business purpose and only to the appropriate person or persons with a need to know.
    b. Employees must use encryption software before e-mailing protected health information identifiable to any consumer. The type of software and instructions on how to use it will be the responsibility of the IT department.
    c. Employees must specifically label any personal E-Mail in the subject line as "Personal" and not use a business signature file. Any messages sent without such labeling may be assumed by the company to have been sent on behalf of the company.

d. Employees must use signature files for business related messages sent to third parties. This makes it clear that the employee is communicating on behalf of the company. In addition, all employees must include the approved security disclaimer as a part of the signature file.

3. Internet and E-Mail Monitoring

a. The company may engage in monitoring of electronic mail messages, internet usage and other electronic files created by employees only in specific instances in which there is good cause for such monitoring or some legal obligation to do so. In such cases, the company shall follow procedures reasonably designed to establish the existence of such cause or obligation and to assure that any monitoring is limited to actions reasonably required under the circumstances. Cause for such monitoring will be brought to the attention of the responsible supervisor and or Director who will conduct or oversee the monitoring.

4. Internet and E-Mail Access

a. Authorized managers and supervisors may access or disclose private electronic messages, internet usage records or files of an employee for any valid business purpose. Employees will be so informed and required to consent to such access as a condition of employment. To ensure understanding and compliance with this policy all employees will be required to show by signature that they reviewed this policy. Employees will be informed of any access or disclosure after the time of such action.

5. New Employee Initiation/Separation.

a. It will be the responsibility of the employee's supervisor to fill out the "New, transferred or Separated Employment Information" form. This is done in the NTSF database which will automatically route the information to HR, IT, Executive Assistant, and Reception. Once received, these departments will add/remove the employee as necessary in their respective systems.

I acknowledge that I have received a copy of policy #02-024 which explains Computer Internet and E-mail use. I agree to read policy #02-024 thoroughly, and ask questions about anything I do not fully understand.

_____ _____

Staff Signature **Date**

_____

Print Full Name

Password Information

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 IT personnel.

Do NOT:
Say your password aloud.
E-mail your password to a co-worker.
Offer anyone hints about what your password might be.

Create a strong password

Strong passwords:

Are eight characters or longer.

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.

Should not 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.

Must contain characters from three of the four classes of characters.

The four character classes are:

1. English uppercase letters (A, B, C).
2. English lowercase letters (a, b, c).
3. Arabic numerals (1, 2, 3).
4. Special characters (!, *, $, or other punctuation symbols).

Passwords must be changed at least every 90 days.