

**Cottonwood, Inc.  
Policies and Procedures**

**SECTION:** Information Technology

**POLICY NO:** 07-004

**SUBJECT:** 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. Internet and E-mail 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 Internet, E-Mail, 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. The 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 Office Manager. Once received, these departments will Add/Remove the employee as necessary in their respective systems.