Revised: 10/2023

Cottonwood, Inc.
Policies and Procedures

SECTION: Information Technology **POLICY NO:** 07-005

SUBJECT: Computer Environment Security

EFFECTIVE DATE: February 1995

Policy:

It is Cottonwood, Inc.'s intent to protect not only the investment in hardware and software but also the data that is stored on both local workstations and Network Servers. The following 3 components will be secured: hardware, software, and all data. It will be the responsibility of the Information Technology Manager (ITM) to develop and implement computer environment security.

Cottonwood, Inc. is now using Microsoft 365, which is a subscription cloud-based version of Microsoft Office, including similar programs, like Outlook, Word Excel and now Teams. Microsoft Teams is cloud-based team collaboration software. Microsoft Teams includes business messaging, calling, video meetings and file sharing. Access to Microsoft 365 products is provided by logging in using Microsoft 365 MFA.

Microsoft 365 MFA (Multi-Factor Authentication) is a method of authentication that requires more than one certification method and adds a second layer of security to user sign-ins and transactions. This method helps safeguard access to data and applications while maintaining simplicity for users. It can use app notifications or text messages on smart phones as the second authentication factor. It is being integrated into the Microsoft 365 environment for all users.

Procedures:

1. **Securing the hardware-** A record of all serial numbers will be kept on file with the ITM. The IT Department will not work on any computers or computer-related equipment not owned by Cottonwood, Inc.

2. **Securing the software-** All software Media will be kept in secure, locked storage. Access to and use of Media will be controlled by the ITM. All programs will be registered appropriately, and the records maintained by the ITM. The program documentation user's manuals, workbooks, etc. will be readily available for the users.

3. **Securing the data-**

   A. All data and working files will be stored on file servers. Only programs will be on the local workstations.

   B. Access to the Network servers will be controlled by login passwords which are to be changed every 90 days. It is against Cottonwood, Inc. policy to post or relay your password to any person other than the IT Department.

C. All computers will have a screen saver password enabled with a maximum 10-minute delay.

D. All Cottonwood, Inc. laptop computers are protected by a hard drive password.

E. Access to each Department's data will be controlled by the Network Security protocols administered by the ITM. The concerned Department Director will determine the need to know for each department. Need to know access for data shared between Departments will be determined by the concerned Directors or Management Team.

F. All data files will be backed up. Incremental (changes only) backups will be done daily. Full back-ups of all files and programs will be done weekly and monthly. Monthly full back-up sets will be stored off-site.

G. Microsoft 365 applications and information utilizes AvePoint Software which provides governance, compliance and management of the platform.

H. Cottonwood, Inc. data will only be accessed through Cottonwood, Inc. network. Software Media is for internal use only and may not be removed from Cottonwood, Inc. premises. All Media from outside sources that are used on the Cottonwood, Inc. network must be scanned for viruses by the ITM or designee prior to use. Employee-owned equipment may not be used to download Cottonwood, Inc. files.

I. A continuous Real Time Virus/Malware scan will be run on the Network Server. This scans all incoming and outgoing files to the server. This scan also detects viruses/malware on network and notifies the ITM.

J. Computers are generally recycled or reconfigured. If a computer is to be sold, taken out of service and recycled, or transferred to another user the hard drive will need to be erased. All computers must have their hard disk drives sanitized (data overwritten) with software that completes a three-pass binary wipe. A three-pass binary wipe writes zeros, ones, and then pseudo-random over existing data. This procedure is completed prior to removing the equipment from the existing environment.

K. Periodically, changes may be made to the network security system with regard to login and password procedures if a security upgrade is felt to be necessary.

L. Cottonwood, Inc. employees must report to a member of management, the ITM, or the Corporate Compliance Officer any knowing or inadvertent violation of Cottonwood Inc.’s security policy. Any violations of the Security policy could result in disciplinary action up to and including termination. The HR Director shall maintain written documentation of disciplinary action in written or electronic form, for six years after the date of its creation or the date when it was last in effect, whichever is later.

M. Security incidents such as the attempted or successful unauthorized access, use, disclosure, notification, destruction of, information or interference with system operations will be mitigated to the extent possible. Incidents will be analyzed as to cause and corrective action taken. This may include employee training, disciplinary action, or system change. (Refer to HIPPA policy #05-050 for information on documentation of a security incident).

N. Cottonwood, Inc.’s Risk Management Plan and Emergency Response Team planning addresses additional areas of back-up and disaster planning.