Revised: 08/2023

Cottonwood, Inc.
Policies and Procedures

SECTION: General **POLICY NO:** 02-016

SUBJECT: Electronic Documentation

EFFECTIVE DATE: March 2015

Policy:

Cottonwood, Inc. has adopted this Electronic Documentation Policy to comply with legal standards requiring authentication of consumer records and the organization's requirement to protect the security, confidentiality and integrity of electronic consumer information.

Procedures:

To safeguard against unauthorized access to the system:

- Logins and passwords are unique to each staff and they may not share their password information and must treat it as strictly confidential. Cottonwood, Inc. requires the password to be changed by the staff person every 90 days. The account will be locked if the password is not changed within the 90-day timeframe. See Policy 07-004.

- Staff are required to log out or lock their computer when it is not in use. When not in use laptops are stored in locked offices or locked drawers to prevent theft which may lead to unauthorized access.

- Every staff is assigned to a specific PC or laptop with a number unique to that staff. In certain departments, computers may be shared.

- The network system maintains an audit trail and timestamp providing details of user names accessing consumer records and/or unlocking consumer records.

- Where necessary internal databases keep logs of which users create/edit/delete individual records in order to provide a database specific audit trail.

- Cottonwood, Inc. IT staff will maintain hardware, server, and network security.

- In the event a staff is terminated from employment, direct supervisors are required to notify IT and HR of the effective termination date by use of the New/Transfer/Separation Form. IT will delete the staff's various user accounts preventing unauthorized access to electronic documentation throughout the Cottonwood, Inc. network.

Cottonwood, Inc.'s security system within Basic Consumer Information (BCI) website protects access to electronic documents through two levels of access control mechanisms with unique identifiers being assigned to each individual user in the system.

- To access BCI, a unique login and password specific to the staff person must be entered to gain access to their customers' information.

- Once the staff person has authenticated into the consumer information area of BCI, only consumers receiving services from Cottonwood, Inc. are available to Cottonwood, Inc. staff.

- The system will reject a user and deny entry into BCI after three (3) attempts at entering the unique login and password information incorrectly. Only Cottonwood, Inc. IT staff are authorized to unlock and allow the staff to gain access into the system. This prevents unauthorized entry into the secured consumer records and ensures that only appropriately identified and password-secured staff are able to access the various applications within BCI.

- The server for BCI is located in the secured server network room of Cottonwood, Inc.

- The server for BCI, including consumer data, is included in the virus protection, daily back up, disaster plan, recovery, and general network security provisions of Cottonwood, Inc.

Enforcement

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline in accordance with Cottonwood, Inc. Policies and Procedures.