Kokua
Support. Encourage. Empower.

TITLE: USE OF AGENCY COMPUTERS

POLICY 3.9

Rev. September 2017

PURPOSE AND SCOPE:
This policy outlines Kokua's expectations for employees in protecting confidential data stored on agency computers.

A. AGENCY GUIDELINES FOR COMPUTER USE
Kokua provides computers for specified employees to be used in the performance of their job duties. All employees will read and sign a copy of this policy (as well as Kokua policy 3.91 and 3.92) to assure that they are familiar with the agency's guidelines for computer use.
Agency computers are to be used for work-related purposes. The following activities are specifically prohibited: use of agency computers for personal gain, to access pornography, to commit an illegal act or to engage in inappropriate conduct, such as harassment. Improper use of agency computers will result in disciplinary action, up to or including termination.
Infrequent or incidental use of an agency's computer that does not interfere with work time or incur a cost to the agency is acceptable.

B. ACCESS TO CONFIDENTIAL DATA
Some agency computers contain confidential information. Access to agency computers containing personnel, financial or client-related data shall be restricted to those individuals designated by the Executive Director. Appropriate measures must be taken when using laptops to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users in order to protect Kokua's client and business information.

C. COMPUTER MAINTENANCE AND SECURITY
Regular computer maintenance will be the responsibility of the Business Operations Coordinator. Employees using computers may not alter the security settings or make changes to the anti-virus software.
The Business Operations Coordinator will keep a master list of all passwords and access codes. This list will be kept in a secured location.

1. Employees must not share passwords with other employees.
2. Employees may not install any unauthorized software onto agency computers; this includes "freeware" available on the Internet.
3. If an employee wants to use a service such as an on-line newsletter that requires the employee to give out their e-mail address, the employee should first get approval from the Executive Director or the Business Operations Coordinator.

D. HOUSE LAPTOP MAINTENANCE AND SECURITY

Appropriate measures must also be taken to reduce the likelihood of physical loss or damage to laptops. Workforce members using laptops shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

Kokua uses the Therap digital documentation software and its associated cloud storage. All staff are required to review and sign policy 3.92 (Therap Usage).

Kokua will implement physical and technical safeguards for all laptops that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Restricting physical access to laptops to only authorized personnel.
- Ensuring laptops are not left unattended in public places on or off Kokua property.
- Securing laptops (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that laptops that were left unsecured will be protected.
- Passwords will be changed every 90 days and will contain at least 8 characters including a mixture of upper and lower case letters, numbers and special characters (i.e. #!%, etc.)
- A software firewall (such as Windows Firewall) should be turned on and configured for the minimal access necessary to perform normal work.
- All operating system and application security related hotfixes, service packs and patches should be applied as early as possible after they have been made available.
- Antivirus software should be kept up to date.
- Laptops are to be used for authorized business purposes only.
- Never installing unauthorized software on laptops.
- All sensitive information, including protected health information (PHI) should be stored in Therap cloud servers only.
- Keeping food and drink away from laptops in order to avoid accidental spills.
- Ensuring that screens/monitors are positioned away from public view.
- When left at Kokua, ensuring laptops are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
- Ensuring, when possible, that all laptops use a surge protector (not just a power strip).
- If wireless network access is used, ensure access is secure by using Therap's encrypted software for all client related work.
- Ensuring laptops are transported and stored in a padded, protective case, bag, backpack, or other similar luggage. Locks should be employed whenever possible.
- When transported by car, laptops should be stowed in the trunk or some other area where it will not be easily seen or attract attention.
- When used away from Kokua office/homes, wireless and Bluetooth should be turned off whenever possible to reduce the likelihood of unauthorized access.
- Public Wi-Fi hotspots should be avoided if at all possible.
- Lost or stolen laptops should be reported to the Executive Director immediately.

Enforcement: Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I have read the above policy and understand the conditions that are expected of me regarding the use of Kokua computers.

____________________________________ _______________________
Employee Signature Date

____
Print Name