



Surveillance Camera Use Policy

Page 1 of 3

Effective Date: 01/01/2020 ; updated 7/2021

Responsibilities: All Employees

Purpose:

This policy sets out the guidelines within which Center for Social change will employ surveillance security cameras. It establishes standards for the installation, viewing, recording, access to, release and destruction of recorded video.

Center for Social Change will employ surveillance cameras to enhance the safety and security of individuals, employees and property, considering individuals reasonable expectation of person privacy. The primary intent of surveillance camera employment is to discourage the occurrence of behavior violating laws or policies and secure evidence that enhances the likelihood of identifying offenders through post incident investigation of incidents and crimes.

The employment of surveillance cameras is a part of an integrated security approach that includes a number of strategies including physical presence of Administrative staff, access controls and alarms. Security cameras may be employed in the front and back of homes, as well as in the common areas within homes to assist with deterring incidents and crime as well as providing evidence should an incident or crime occur. No surveillance camera use will be in place within private areas of the homes, to include bedrooms or bathrooms

Policy:

It is the policy of Center for Social Change that video surveillance, recording, viewing and release will be handled in accordance with Federal, State, and Local guidelines; and in accordance with all HIPPA privacy rights, rules and regulations.

Procedures:

1. Installation

The COO or CEO of Center for Social Change will approve the installation and the appropriate placement of surveillance cameras and ensure all team members for each individual receiving service at each location is aware of the use of such surveillance. Each individual will also be aware of the surveillance camera use. No surveillance camera will be placed in or upon any program without the authorization of the COO or CEO. Center for Social Change will maintain a record of each authorized camera location. Surveillance cameras employed by Center for Social Change in all programs are limited to video recording capabilities only. No audio surveillance can be detected or recorded by these cameras.

Any new cameras that receives approval to be installed must connect to the Center for Social Change's Network Video Recorder (NVR) system, which will be maintained by Information Technology Services (ITS).

Cameras will not be installed in areas where individuals and staff could reasonably expect privacy, such as restrooms and bedrooms.

2. Signage

In all homes where surveillance cameras are installed, signs must be displayed indicating that an area may be recorded, in compliance with signage requirements under relevant laws and regulations before live camera recording without audio may begin. Signage shall serve as the method to inform all individuals, employees and visitors of surveillance camera installation. Signage states that surveillance cameras are in use, not that they are being monitored. Monitoring implies 24-hour viewing of live footage.

3. Viewing

Viewing of surveillance camera footage (either live video feed or recordings) will be conducted by authorized Center for Social Change's personnel as designated by the COO or CEO. Center for Social Change will ensure that administrative personnel and other designated individuals involved in any live camera monitoring will perform their duties in a legal, responsible and ethical manner. Administrative personnel and other designated individuals viewing live footage or conducting investigations of stored footage from the Network Video Recorder System will not discuss any information, contained within or regarding the footage, to any individuals outside of their chain of command. All designated individuals viewing live feed and/or reviewing recorded video footage will be required to sign a confidentiality agreement to prevent unauthorized disclosure.

Surveillance camera viewing does not guarantee that someone on agency property is safe from crime. There should not be an expectation that the surveillance cameras are being monitored 24 hours, seven days a week and that Center for Social Change is going to observe and respond to a crime in progress.

4. Access and Release

Only the COO and CEO of Center for Social Change will have access to all real-time and recorded images resulting from video surveillance employment. Only authorized members of Center for Social Change may review surveillance camera recorded data via authorization approved by the COO or CEO. Other individuals who may have a legitimate need to view recorded video data may be permitted to do so, but only with the prior approval of the COO or CEO. Circumstances that may warrant a review should be limited to instances where an incident has been reported/observed or for investigation of a potential crime or incident. A request to review recorded footage must be submitted in writing, utilizing the PSD Surveillance Footage Request Form to the COO or CEO. All viewing will be recorded on a log, identifying the need to review the recording, the individuals present, the location of the footage being viewed and the date. The log will be maintained for a period of 12 months and is located within the office of the COO/CEO.

Requests from any entity to release or obtain a copy of recorded data must be authorized by the COO or CEO. Recorded data may be released when it is related to a criminal investigation, civil suit, subpoena or court order, arrest, or to disciplinary proceedings against an employee or personnel actions against an employee. Any release of recorded data will be reflected on a written log.

5. Storage and Retention

Recorded surveillance camera data will be retained for a minimum of 30 days (could be longer as NVR storage capacity increases) unless required for a continuing investigation of an incident, after which the recorded data will be erased or destroyed. All recorded data will be stored on assigned secure network video recorders with secured access. Recorded data retained for investigation purposes will be strictly managed with limited access.