

**Public Works Department Surveillance Technology Use Policy for Illegal Dumping Surveillance Cameras**

**A. Purpose**



*FY20-21 Illegal Dumping Work Orders Completed by KOCB*

Illegal dumping is an epidemic in Oakland. The City is resolved to turn the tide on the widespread dumping by holding violators accountable. But as personnel necessary to deter dumping are limited, surveillance cameras offer the City a viable way to enhance/ support the investigative work performed by Oakland Public Works’ (OPW’s) four Environmental Enforcement Officers (EEOs). This Use Policy is for the operation of the POD – a surveillance system by Security Lines U.S.

The goal of installing POD units near chronic dumping hot spots is to capture video evidence that identifies dumpers or produces supporting information needed to build credible cases for prosecution.

Staff believes there will be an immediate chilling effect on illegal dumping once the City prosecutes more cases using video evidence. Dumpers will have to re-evaluate their desire to dump against the higher risk of getting caught. Over time, surveillance cameras may serve as an ongoing, visual deterrent to potential dumpers after the surveillance program matures.

**B. Authorized Use**

Authorized use of the POD surveillance system:

- surveilling illegal dumping activity in the City of Oakland

Only staff with a need-to-know and a right-to-know will have access to recordings captured by the POD system. See sections **D. Data Access**, and **H. Third Party Data Sharing**, for a list of individuals who will be authorized to access and/or view surveillance data.

### C. Data Collection

Data collection occurs inside a POD housing unit near chronic illegal dumping hot spots. Video captured from the cameras are recorded directly to the digital video recorder's (DVR's) hard drive (2 TB SATA). DVRs do not possess artificial intelligence (AI) or analytics such as facial recognition. The POD surveillance system does not connect to the Cloud.

### D. Data Access

There are three different levels of security to safeguard access to the video data.

1. Cellular router level: An authorized user's computer must be recognized by the cellular router ("Router") before s/he can gain access to the POD system. Personnel with "admin/super user" profiles will specify which computers' IP addresses the Router recognizes. A unique username/password is required to configure the Router.
2. Desktop software level: To interface with the POD system, proprietary POD software will be installed on an authorized user's computer. A unique username/password is required to access software. Different levels of POD access – view only, PTZ camera control, video search & download, and admin/super user access – may be assigned to different personnel by the admin/super user.
3. DVR level (for **optional** mobile phone application only): Each POD has its own DVR. To access a specific POD's recordings, a separate username/password is required to access the DVR associated with that POD. Like the desktop software, users may be added or removed and given different levels of access.

The City of Oakland has sole access to POD video data. Vendor Security Lines U.S. cannot access nor control POD units installed by their clients. The POD surveillance system does not connect to the Cloud. Furthermore, OPW will assign "occasional, as-needed" users with view only access, while select Environmental Enforcement Unit personnel will be granted view and PTZ control access, as well as clearance to search and download video footage. Finally, OPW will limit admin/super user access with the ability to add/delete users to two OPW personnel.

Individuals authorized to access and/or view surveillance camera information include:

Oakland Public Works –

- KOCB Operations Manager, who oversees the EEU, will be able to add/delete users and will be granted admin/super user access.
- OPW Bureau of Environment's Administrative Services Manager, who oversees the Illegal Dumping Surveillance Camera Use Policy, will be able to add/delete

users and be given admin/super user access.

- Environmental Enforcement Unit (EEU) Supervisor and EEU Administrative Analyst, who will be tasked with checking cameras for illegal dumping activities and remote monitoring the POD units, will be given access to view video, control PTZ cameras, as well as search and download video evidence. EEU Supervisor and EEU Administrative Analyst will not have the ability to add or delete users.
- EEOs who investigate illegal dumping cases will be viewing and handling select video clips to gather and package evidence for the OCA. Security access to the POD system may be granted based on operational needs.

## E. Data Protection

Since its introduction in 2009, the POD surveillance system has never been hacked. POD DVRs are Linux-based. Downloaded video is encrypted. Video recordings cannot be played using standard video players (e.g., Windows Media Player). Please refer to section **D. Data Access** for the multi-level security measures required to access POD systems.

## F. Data Retention

There are 2 ways video data are retained.

1. DVR hard drive: The POD DVR records video to the hard drive housed inside the POD unit. The hard drive automatically overwrites the oldest recordings. Routine video recordings not downloaded will be purged automatically and permanently by the DVR every 14 days, when new video is saved on top of the oldest recordings.
2. Downloaded video: Video will only be downloaded when it contains adequate evidence of illegal dumping to warrant possible enforcement actions. An authorized user will download the video clips via the POD desktop software to a secure OPW folder. Downloaded recordings will be purged once filed claims, pending litigation, and/or criminal investigations and prosecutions conclude.

## G. Public Access

Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

## H. Third-Party Data Sharing

There is no third-party data sharing with the POD surveillance system. The vendor cannot access the City's video data through the POD software. Computers with IP addresses entered by the City's admin/super user are the only computers permitted to access the PODs. (See section **D. Data Access**) The POD surveillance system does not connect to the Cloud.

Other City departments or non-City entities that may view or use POD video recordings are:

### City Attorney's Office (OCA) –

- Assigned City Attorney staff in OCA's Litigation Division will view select video clips 1) to ascertain the viability of the video evidence, and 2) to work up a case to initiate legal actions to prosecute the dumper for violations of the Oakland Municipal Code. Security access to the POD system is not required.

### Administrative Hearing Officer –

- Assigned Administrative Hearing Officer may view select video clips in the course of adjudicating illegal dumping cases via the City's administrative hearings (due process hearings for violators that appeal the City's determinations on violations). Security access to the POD system is not required.

### Oakland Police Department (OPD)/ Alameda County District Attorney's (DA's) Office –

- In the event POD cameras capture illegal dumping of the scale and/or nature that warrant criminal investigations, EEU staff may share select video clips with OPD and/or the DA's Office for further illegal dumping investigatory and enforcement actions. Security access to the POD system is not required.

## I. Training

Training is available in video tutorials and written formats on vendor Security Lines U.S.'s website in a members-only area. One on one remote training is available. The Administrative Services Manager in OPW's Bureau of Environment shall conduct training with authorized POD users. Training will include reading this Use Policy and reviewing operational procedures required to adhere to the Policy.

## J. Auditing and Oversight

The Administrative Services Manager in OPW's Bureau of Environment shall conduct annual assessments to ensure authorized users comply with the Use Policy.

All POD user and device activity are logged. Designated admin/super users can access and view audit logs at the camera level. The audit log tracks system access and ties

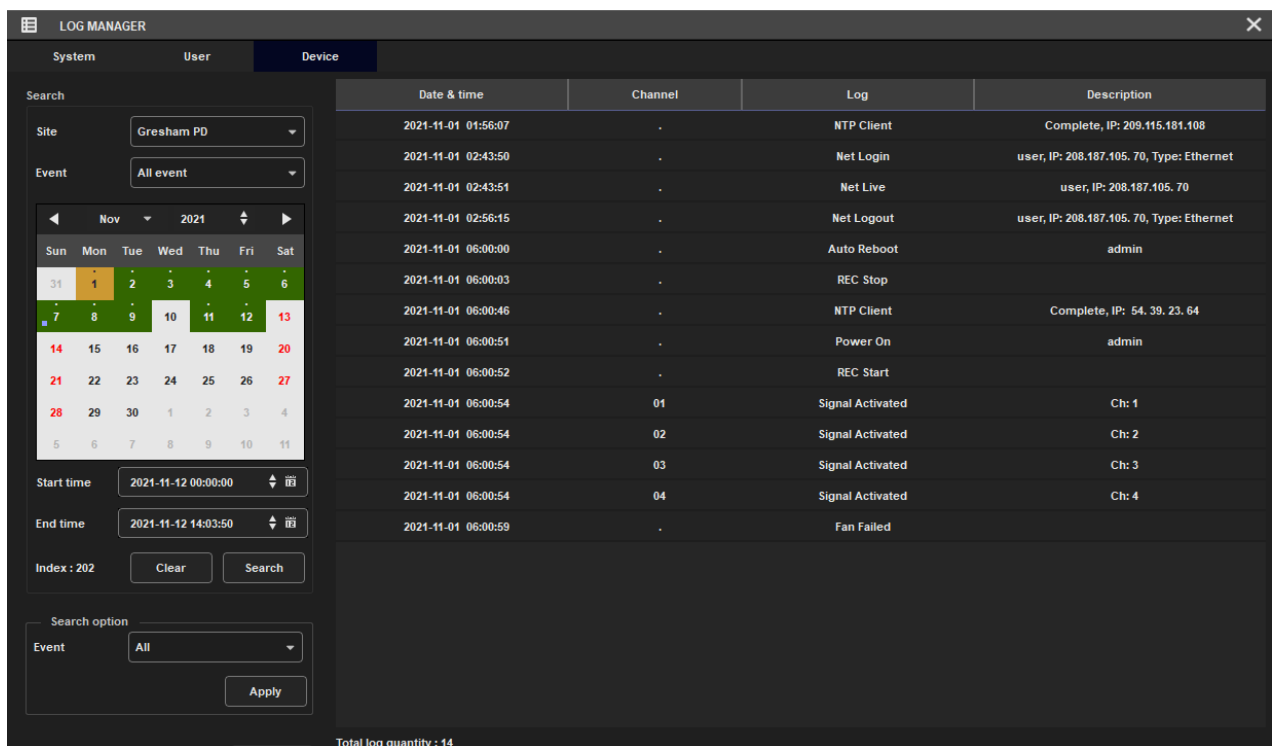
each action to a user for events such as:

- User Log-ins/ Log-outs by IP address
- User Management (add, edit, delete users; settings imported/exported)

The audit log also tracks device-specific events such as:

- Recordings stopped and started
- Reboots
- Power On
- Time syncs

*Example of audit log.*



The screenshot displays the 'LOG MANAGER' interface. On the left, there is a search sidebar with filters for Site (Gresham PD), Event (All event), a calendar for November 2021, Start time (2021-11-12 00:00:00), End time (2021-11-12 14:03:50), and Search options. The main area shows a table of log entries with columns for Date & time, Channel, Log, and Description.

Date & time	Channel	Log	Description
2021-11-01 01:56:07	-	NTP Client	Complete, IP: 209.115.181.108
2021-11-01 02:43:50	-	Net Login	user, IP: 208.187.105. 70, Type: Ethernet
2021-11-01 02:43:51	-	Net Live	user, IP: 208.187.105. 70
2021-11-01 02:56:15	-	Net Logout	user, IP: 208.187.105. 70, Type: Ethernet
2021-11-01 06:00:00	-	Auto Reboot	admin
2021-11-01 06:00:03	-	REC Stop	
2021-11-01 06:00:46	-	NTP Client	Complete, IP: 54. 39. 23. 64
2021-11-01 06:00:51	-	Power On	admin
2021-11-01 06:00:52	-	REC Start	
2021-11-01 06:00:54	01	Signal Activated	Ch: 1
2021-11-01 06:00:54	02	Signal Activated	Ch: 2
2021-11-01 06:00:54	03	Signal Activated	Ch: 3
2021-11-01 06:00:54	04	Signal Activated	Ch: 4
2021-11-01 06:00:59	-	Fan Failed	

## K. Maintenance

Security Lines U.S. offers but does not require a maintenance contract. The POD's simple, rugged design requires minimal maintenance. Vendor and existing client testimonials suggest that maintenance, when required, constituted the occasional replacement of a hard drive or camera cover, which most client organizations service themselves.