Surveillance Use Policy
PENLiNK PLX
San Diego Police Department

PURPOSE

PENLiNK PLX is computer software available to local, state, federal, and international law enforcement agencies. As defined on PENLINK.com, the software provides, "digital investigative solutions bringing innovative analytical capabilities to reveal connections and gain insights more quickly. Combat job fatigue and burnout with PLX and its powerful, easy-to-use, and flexible array of reporting and analytical tools to help reveal connections, trends, and relationships that might otherwise go undetected. With options for interactive grids, graphical analysis, and reporting across phone calls, messaging, social media, and more, PLX does in minutes what would take investigator weeks to do manually." It offers San Diego Internet Crimes Against Children Task Force (ICAC) members the ability to examine large data sets obtained through legal processes in one integrated view. The program parses out information and organizes it in a manner that is useable and logical allowing task force members to more efficiently review, oftentimes, terabytes of information. It is used to support ICAC criminal investigations.

USE

PENLiNK PLX is utilized by ICAC members for investigative purposes. The program is only accessed by authorized task force members after receiving data from electronic service providers as a result of a legal process being served. Utilizing this database enhances and expedites the investigative process.

DATA COLLECTION

Data provided by electronic service providers as a result of a legal process being served is uploaded onto an isolated computer. The PENLiNK PLX program, using proprietary software coding, parses out the data into usable, logical files (e.g., images, videos, emails, and text messages). Investigators then review the organized data and determine the evidentiary value of what was received. When the review is complete, PENLiNK PLX will produce a report indicating the items selected. The task force member validates the authenticity of the information through the appropriate custodian of records through the service of legal processes. That report is then provided to the prosecutor as part of a much larger investigation.

DATA ACCESS

Only task force members, investigators, and certified forensic examiners, who have been trained and certificated by PENLiNK and have been authorized by the task force commander to perform analysis may use PENLiNK PLX.

When accessing PENLiNK PLX, the user enters a case number or other unique identifier associated with the related law enforcement event in the "Reference ID" field.

DATA PROTECTION

PENLiNK PLX software is stored and maintained in ICAC, a secured office located away from Police Headquarters. Only authorized users have access to the office space and technology.

PENLiNK PLX software is not located on a department network computer and can only be accessed by logging in to the computer with the software. The computer has no internet access and is not accessible by the vendor. Additionally, the software can only be installed through a specific process, it cannot be moved, and the user must be an authorized user with a valid software license. The PENLiNK PLX software cannot be accessed outside of the task force.

DATA RETENTION

Per evidence code sections related to crimes perpetrated against children allowing for historical evidence to be brought forth, analyzed data is retained until the death of the suspect.

PUBLIC ACCESS

The data analyzed using PENLiNK PLX technology is only used in criminal investigations and is not available to the public. Copies of the data can only be obtained with a court order or through the discovery process.

THIRD-PARTY DATA SHARING

Data analyzed and organized using PENLiNK PLX technology is not shared without a court order or other legal proceedings such as discovery. The extracted data is considered confidential, and there is no third-party access or sharing. The vendor does not have access to the extracted data.

TRAINING

Investigators and certified forensic examiners who use the PENLiNK PLX software must complete a training program provided by PENLiNK PLX before using the software.

AUDITING AND OVERSIGHT

An audit of PENLiNK PLX can be performed by site administrators (ICAC Task Force Commander) on an as-needed basis. Users who leave the task force have their access removed. At the point of conducting an inquiry, a field titled "Reference" serves as a method to demonstrate the user's "need to know, right to know" by providing case numbers, incident numbers, or other unique identifiers.

Misuse of the system would be reported to and investigated by the task force member's Internal Affairs unit. Violations of the laws, agency policies, or user agreement terms and conditions would subject the task force member to discipline and/or criminal proceedings or civil processes.

MAINTENANCE

The PENLinK PLX software is controlled and maintained by the vendor and ICAC. The ICAC commander is responsible for monitoring and updating software when new versions are released.