

County of Santa Clara

Probation Department Surveillance Use Policy

Electronic Monitoring Program Devices (Global Positioning System, Radio Frequency, & Alcohol Monitoring Devices)

1. Purpose

The Santa Clara County Probation Department's Electronic Monitoring Program (EMP or EMP systems) includes the use of Global Positioning System (GPS) devices, Radio Frequency (RF) devices, and Alcohol monitoring devices, all of which shall be used pursuant to and in compliance with court orders. GPS, RF, and Alcohol monitoring devices are electronic transmitters that are attached to a person's ankle for court-ordered monitoring, as an alternative to serving custody time in juvenile hall or jail.

The (GPS) monitoring devices (currently Attenti WMTD Gen 4 GSM/ Attenti WMTD Gen 4 CDMA/ BI loc8) are designed to track the movement of a person for extended periods of time. The device uses standard GPS technology, whereby it identifies the person's location by coordinating with multiple GPS satellites. GPS is capable of updating a location every ten seconds and pinpointing location to within inches.

The (RF) monitoring devices (currently Attenti SB2000 RF/ SB3000 RF/ BI HomeGuard 200 (HG200)/ BI HomeGuard 206 (HG206)) send a signal to a Field Monitoring Device (FMD) receiver installed in a person's home. That FMD is in contact with the host network via telephone lines and modem. The RF device logs the person's movements in and out of their home.

The Alcohol monitoring devices (currently SCRAM CAM / SCRAM Remote Breath/ Soberlink-SL2) use standard GPS or RF technology to either read a person's location or log a person's movements in and out of their home. In addition, one alcohol monitoring device has a handheld portable breathalyzer, which allows a person to discreetly submit a Breath Alcohol Test from any location using cellular service. The second alcohol monitoring device is a transdermal alcohol monitoring device, which tests and reports alcohol consumption based on readings through the skin.

Information collected by GPS, RF, and Alcohol monitoring devices are streamed from the host networks to a web server operated by the host companies.

2. Authorized and Prohibited Uses

The EMP systems shall be used only for the purposes of the court-ordered electronic monitoring described in Section 1 of this Policy. The Chief Probation Officer and the Chief's designees shall administer and monitor the EMP systems, including granting access to monitor and review data collected by the EMP systems to Probation

Department peace officers or Information Technology staff assigned specifically to this task.

The EMP systems and the data collected and stored shall be used for only lawful monitoring of a person's location and/or activities in accordance with court-ordered monitoring, for the following purposes:

- To assist in the monitoring of an offender's compliance with court orders;
- To assist in the identification and prevention of threats;
- To assist in identifying, apprehending, and prosecuting offenders;
- To assist in gathering evidence for criminal and probation court actions;
- To assist in resolving a citizen or employee complaint, internal affairs investigation, or other county or law enforcement investigation; or
- As otherwise permitted by state law, under California Penal Code Section 1203.016.

The Department's EMP systems shall be used in a legal manner. The EMP systems shall not be used to harass, intimidate, or discriminate against any individual or group.

The EMP systems (GPS, RF, and Alcohol monitoring devices) shall not be used in an unauthorized manner, for personal purposes or for any unauthorized purpose.

3. Data Collection

GPS monitoring devices within the EMP systems shall collect and store location/movement data regarding the wearer of the device. The devices update frequently as described in Section 1 of this Policy, and pinpoint location within inches.

RF monitoring devices within the EMP systems shall collect data regarding the in-home and out-of-home movements of the wearer of the RF devices, including curfew violations, missed call-backs, tampering, location failures, FMD disconnects, and power loss.

Alcohol monitoring devices within the EMP systems shall collect data regarding the location and movement of a person. In addition, the alcohol monitoring device with a handheld portable breathalyzer shall collect data on alcohol consumption, take and store photographs, and use facial recognition to assist in verifying the user. The alcohol monitoring device with transdermal alcohol monitoring technology shall collect data on alcohol levels/consumption.

//

4. Data Access

Only authorized personnel shall access GPS, RF, and Alcohol monitoring data. Specifically, the Chief of Probation, Deputy Chief Probation Officers of the Juvenile Institutions Division and Adult Services Division, Probation Executive Management designated by the Chief of Probation, peace officers designated by the Chief of Probation, and Probation Information Technology staff members shall be authorized to access data from the EMP systems for Probation business purposes only, pursuant to a court order. To the extent the vendor/hosting company for the technology have data access, they shall be required to keep the data confidential. Efforts shall be made to keep the total number of designees with access to the data as low as possible within the constraints of this Policy.

5. Data Protection

GPS, RF, and Alcohol monitoring data shall be stored on secured, dedicated servers that are protected from intrusion by the host companies' network security and encryption services. The vendor/host company for the data management shall be required to maintain security measures to maintain client and program security and confidentiality, including by 24/7/365 monitoring of the data centers and by limiting access to only designated personnel. Probation Department access to those systems shall be through secure-access measures, which shall include passwords and encryption.

Monitors for viewing GPS, RF, and Alcohol monitoring data shall be in secured areas that prevent viewing by unauthorized staff members and the public.

6. Data Retention

Physical backups of data shall be made by the host companies. These backups, which shall include both active and inactive clients' records, shall be stored for up to seven years. However, specific data shall be retained for a longer time if that data is used as part of a specific administrative or criminal investigation or prosecution for which the data serves as evidence, or for official reasons in the normal course of Probation business.

7. Public Access

The public shall not have direct access to data collected or retained from the GPS, RF, or Alcohol monitoring technology, but the public may access data in court that is presented in court in a public criminal proceeding or that becomes a part of a court file that is accessible to the public. If a California Public Records Act request, subpoena, or court order is issued for the data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Office of the County Counsel as necessary to ensure legal compliance.

//

//

8. Third-Party Data-Sharing

As part of the court process, data shall be shared with the court, the District Attorney, and counsel for the individual who is subject to the monitoring order. Other third-party data-sharing shall be prohibited unless consent is obtained from the Chief Probation Officer or the Chief's authorized designee for a specific administrative or criminal investigation or prosecution; or a law or court order mandates third-party data-sharing.

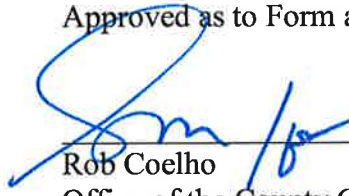
9. Training

Personnel involved in using or accessing GPS, RF, or Alcohol monitoring equipment and data from the EMP systems shall be trained regarding the technology and shall be given a copy of this Policy.

10. Oversight

The Deputy Chief Probation Officers of the Juvenile Institutions and Adult Services Divisions shall oversee compliance with this Policy. Only valid users with an authorized identification and password shall have access to monitor and review data in the systems. (See, e.g., Section 4 of this Policy). Access and activity logs shall be maintained regarding access to data. Any employee found to have violated this Policy shall be subject to discipline, up to and including termination.

Approved as to Form and Legality



Rob Coelho
Office of the County Counsel