Santa Clara County Office of the Sheriff
Inmate Tablet Monitoring
Surveillance Use Policy

Santa Clara County
Sheriff's Office
Custody Bureau

1. Purpose

The Inmate Tablet Services Platform (ITSP) provided by Legacy Long Distance Int'l Inc. (Legacy) records inmate tablet activity, which is monitored to assess safety and security issues within jail facilities. ITSP has an optional feature for inmate messaging, which shall not be enabled until Legacy provides a technological solution to ensure that Privileged Communication is not recorded or monitored by the County or Sheriff's personnel. To monitor tablet activity, Legacy will provide the Office of the Sheriff's administrative accounts with access to a mobile device management system. This system shall be used to help the Sheriff's Office assess risk to the Correctional Facilities based on information shared by inmates during messaging that indicate security violations of inmates, introduction of contraband, escape plans, intentions to attack staff or others, attempts to direct, control, or participate in criminal behavior, or plans to adversely impact the jail's operation.

2. Authorized and Prohibited Uses

A Monitoring/Recording notice shall be prominently displayed on the tablets advising inmates that their tablet usage is being monitored or recorded.

A. Authorized uses for the mobile device management system shall include only the following:

1. <u>Tablet Management</u>

    a. Remote lock/disable device
    b. Remote Device Wipe
    c. Device Factory Reset
    d. Application Install and Removal
    e. Control Network Access
    f. Reassignment of Device to New User
    g. Emergency Shutdown
    h. Equipment Upgrades
    i. App Upgrades

2. <u>Inmate Messaging Internal Controls</u>

    a. *Translation* - automatically translate inmate messages or requests into English
    b. *Flagging* - flag hot words, even misspellings, with e-mail or admin portal notifications
    c. *Quarantines* - block messages with hot words like "escape" before they are sent
    d. *Link Analysis* - analyze connections to external contacts and other inmates
    e. *"Cut & Paste" detection* - prevent or flag communication through outside sources with detection of messages cut and pasted to other recipients
    f. *Filtered Searches* - limit any search to a specific location or charge

3. Tablet Monitoring

   a. Listening to or monitoring in-progress ITSP calls and messaging
   b. Reviewing recorded ITSP calls and messaging
   c. Evidence collection from tablets
   d. Other law enforcement, custody, or first responder uses not prohibited by law

B. All uses not authorized above shall be prohibited. The mobile device management system shall not be used for personal or non-official purposes. It shall be used in a legal manner, and shall not be used to harass, intimidate, or discriminate against any individual or group.

C. The Sheriff's Office shall not listen to, read, or record a communication known by the listener, reader, or recorder to be privileged. Privileged communication shall be defined as attorney-client communication, physician-patient communication, and clergy-penitent communication. Any inadvertent recording of a privileged communication (e.g., a communication by an inmate to the inmate's attorney) shall be deleted upon discovery and if the recording has been copied, all copies shall be deleted immediately.

D. If communication is made to the Adult Custody Office of the Ombuds (ACOO), formerly known as the Jail Observer Program, the communication shall not be observed, listened to or recorded.

3. Data Collection

A. It shall be permissible for the following data to be obtained through the mobile device management system for each tablet:

   a. Monthly Usage Reports by inmate or facility
      - Courses completed
      - Certificates Issued
      - Points Earned
      - Peak Usage Times
   b. Inmate's User Identification
   c. User activity
      - Content Viewed
      - Progress on educational components

- Aggregate Tablet Usage information

d. Number dialed by the inmate

e. Duration and content of call or messaging

f. Exact tablet the call or message was placed on

g. Submission details and tracking for Grievances, Requests, and Commissary Orders

h. Actions taken by Sheriff's Office administrative users to limit or restrict inmate access

4. Data Access

Access to the mobile device management system data shall be limited to authorized Sheriff's Office personnel in writing, which includes the Sheriff's Classification Unit, Intel Unit, Programs Unit, Facility Commanders, Sheriff's personnel conducting a specific criminal or administrative investigation; and the vendor (Legacy) for only the purposes of maintaining their system (maintenance, updates, quality control, etc.).

5. Data Protection

The County's contract for tablet monitoring shall require that data from the mobile device management system shall be maintained securely. Currently, Legacy provides secure hard drives located at its Cypress headquarters, to securely store all data captured by the mobile device management system. The data shall be made available to the Classification Unit through a secure web-based management portal, hosted by Legacy. All authorized staff with access to the Legacy management portal shall observe all required security measures to ensure that access to the mobile device management system is limited to authorized personnel only.

6. Data Retention

Audio recordings stored on the mobile device management system hard drives shall be retained for no longer than two years. At that point, the Legacy management portal shall purge the information. For a specific criminal or administrative investigation, it shall be permissible for data to be downloaded onto an electronic storage device for the purposes of documentation or evidence. Downloaded and copied data shall be maintained in accordance with applicable state and federal laws, and shall be retained as long as deemed necessary for administrative or criminal investigation and prosecution purposes. All other data shall be retained for no longer than two years.

7. Public Access

Inmate mobile device management system data shall not be released to the general public. Data utilized as evidence in a criminal case may be made public during the course of a public jury trial or pursuant to a Court Order, but shall otherwise remain confidential.

8. Third-Party Data-Sharing

A. With respect to Third-Party Data Sharing, data from the Inmate Tablet Services Platform mobile device management system shall require the submission of a Sheriff's Office Request Form or subpoena.

B. The Sheriff's Office Request Form shall include:

1. Date/time
2. Requesting agency
3. Name of requesting officer
4. Associated case number
5. Inmate name and CEN/Booking number
6. Range of dates to search
7. Receiving party's telephone number(s)
8. Reason for request

C. The Request Form shall be reviewed and, if approved, signed by the Classification Lieutenant, Captain, or designee approved in writing by the Sheriff.

D. It shall be permissible for inmate messaging data to be shared with only the following:

1. District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence
2. Public Defender's Office or criminal defense attorney via the District Attorney's Office pursuant to California discovery laws
3. Other law enforcement offices as part of a specific criminal or administrative investigation
4. Parties to civil litigation involving the County, in response to a subpoena or civil discovery
5. County Personnel Board, arbitrator, or Court regarding a county administrative action or litigation
6. Other third parties, pursuant to a Court Order

9. Training

Training for the mobile device management system shall be provided by Sheriff's Office personnel and shall be limited to Sheriff's Office personnel authorized to access the Inmate Tablet Services Platform device management system and its data. All Sheriff's Office

personnel with access to this equipment shall be provided a copy of this Surveillance Use Policy.

10. Oversight

The Support Services Captain shall ensure the Inmate Tablet Services Platform mobile device management system is used in compliance with this Surveillance Use Policy. Sheriff's supervisors or administrators shall conduct audits of the system as necessary and at least annually to ensure appropriate use within the directives of this Surveillance Use Policy. The results of non-privileged audits shall be shared with the County of Santa Clara Board of Supervisors in the Annual Surveillance Report provided by the Sheriff's Office each year. If there are privileged audits conducted that reveal any violation of this policy, then the Sheriff or designee shall notify the Office of the County Counsel, and such results may be shared as part of an attorney-client communication to the Board of Supervisors, including in closed session if lawful to do so, at the request of the Board of Supervisors.

Approved as to Form and Legality

10/18/19

Rob Coelho
Office of the County Counsel