1. **Purpose**

Investigators in the Santa Clara County District Attorney’s Office (SCCDA) utilize a variety of data extraction/examination forensic tools and software to extract, process, enhance, and analyze data from various types of digital devices, including computers, cellular phones, tablets, thumb drives, audio equipment, and video equipment, associated with the investigation of a criminal activity.\(^1\) The data retrieved using the tools and software includes computer files, e-mails, contacts, digital images, audio and video files, and other multimedia files. The extracted data may be relevant to prove, among other things: 1) whether criminal activity has occurred or is occurring; 2) the identity of the person involved in the criminal activity; 3) the intent or motive of the person involved in the criminal activity; and 4) applicable legal defenses to the suspected criminal activity.

2. **Authorized and Prohibited Uses**

Use of data extraction/examination forensic tools and software shall be limited to SCCDA personnel authorized by SCCDA Administration to use solely in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA. Data extraction/examination forensic tools and software shall only be utilized pursuant to judicial authorization; with valid consent; or in circumstances that, under the law, do not impact anyone’s reasonable expectation of privacy. When the use of data extraction/examination forensic tools and software requires a search warrant, the assigned investigator and/or prosecutor shall make an application to the court and obtain court approval before using the equipment. In cases where the use of data extraction/examination forensic tools and software is not governed by a search warrant or other court order, the user shall abide by this Surveillance Use Policy.

County-owned data extraction/examination forensic tools and software and associated data shall not be used for personal, non-SCCDA purposes. The equipment shall not be used for illegal purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

\(^1\) To promote officer safety and maximize the benefits to be derived from the use of data extraction/examination forensic tools and software, the specific make and model of the devices owned by the SCCDA have been omitted from this Surveillance Use Policy.
3. **Data Collection**

The tools have the potential to access a wide range of data on digital devices, including personal and sensitive information. Depending on the specific forensic tools and software, authorized personnel shall create a forensic image of a digital device when possible to avoid alteration or destruction of the evidence. Forensic tools and specialized software and applications shall only be used to recover, enhance, and analyze data from legally-acquired devices and sources in compliance with applicable federal, state, and local laws, as well as this Surveillance Use Policy. Collected data that is downloaded shall be retained in a secure file.

4. **Data Access**

The data collected by extraction/examination forensic tools and software shall be stored in the physical case file and/or stored within an SCCDA-approved electronic case/content management system. Approved case/content management systems shall log user name, date/timestamp, files or data accessed, and attempts at altering or deleting files. Access to the data generated through the use of extraction/examination forensic tools and software shall be limited to only SCCDA personnel authorized by SCCDA Administration to utilize the data in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA, as well as other county personnel designated in writing by the District Attorney or the District Attorney’s written designee to the extent that access is necessary for a specific criminal, civil, or administrative investigation or action.

5. **Data Protection**

See Sections 3 and 4 of this Policy. The County of Santa Clara and the SCCDA shall utilize physical access controls, application permission controls, and other technological, administrative, procedural, operational, and personnel security measures to protect data collected by extraction/examination forensic tools and software from unauthorized access, destruction, use, modification, or disclosure.

6. **Data Retention**

Data recovered through the use of extraction/examination tools and software, whether downloaded, copied or printed, shall be maintained in accordance with this Surveillance Use Policy, applicable state and federal evidentiary laws, and the SCCDA Record Retention and Destruction Policy approved by the Board of Supervisors on June 21, 2016, as follows:

<table>
<thead>
<tr>
<th>Case Type</th>
<th>Official Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homicide Case Files</td>
<td>Permanent</td>
</tr>
</tbody>
</table>

Office of the District Attorney Surveillance Use Policy – Data Extraction/Examination Tools and Software
<table>
<thead>
<tr>
<th>Case Type</th>
<th>Official Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Non-Homicide Case Files, Unless Otherwise Stated in this Schedule</strong></td>
<td>Seventy-five years. Case files will be scanned and electronically archived and retained for 75 years. Originals will be retained for a period of at least 90 days to allow scanning for authentication by the department, after which they will be destroyed. Backed up by DA IT provider.</td>
</tr>
<tr>
<td><strong>Juvenile Ward Files</strong></td>
<td>When a minor turns 18 and petitions the court for records to be sealed, the record will be destroyed at age 20 or as otherwise ordered by a court of competent jurisdiction. Otherwise as covered by this schedule.</td>
</tr>
<tr>
<td><strong>Developmentally Disabled (DD) Case Files</strong></td>
<td>Life of the defendant.</td>
</tr>
<tr>
<td><strong>Plea of Insanity (PC 1026) Case Files</strong></td>
<td>Life of the defendant.</td>
</tr>
<tr>
<td><strong>Juvenile Case Files</strong></td>
<td>Two years after final disposition or until minor attains age of 21, whichever is later. Caveat 1): If case is appealed, the file must be retained until the final appellate decision is received. Caveat 2): Cases that may be charged as “strikes” should be retained for 75 years.</td>
</tr>
<tr>
<td><strong>Certificates of Rehabilitation Case Files</strong></td>
<td>Two years.</td>
</tr>
<tr>
<td><strong>Advise and Assist Case Files</strong></td>
<td>Two years.</td>
</tr>
<tr>
<td><strong>Expungement Case Files</strong></td>
<td>Two years.</td>
</tr>
<tr>
<td><strong>Post-Conviction Proceedings and Special Project Files</strong></td>
<td>Two years.</td>
</tr>
</tbody>
</table>
Data that is relevant to administrative/personnel-related matters shall be retained through the adjudication of any administrative, civil or criminal case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations. To the extent that data is not covered in the chart above, the data shall be destroyed no later than two years after the later of (1) the time for an appeals process expires; (2) the statute of limitations expires; and (3) for data regarding a County employee’s administrative investigation, the date the employee’s employment for the County terminates.

7. Public Access

Absent a court order, the public shall not have direct access to data collected by data extraction/examination forensic tools and software. If a California Public Records Act (CPRA) request, subpoena, or court order is issued for this data, it 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 needed. It is likely that the District Attorney’s Office shall deny CPRA requests for forensic images or recovered data on the ground that such images and data are exempt from disclosure under at least the investigative exemption (Government Code section 6254(f)) to the CPRA.

8. Third-Party Data-Sharing

The sharing of data recovered through the use of data extraction/examination forensic tools and software shall be limited to the following third parties:

- Law enforcement agencies when relevant to an ongoing specific investigation or prosecution;
- Defense and appellate counsel and pro se litigants pursuant to Penal Code section 1054 et seq. and Brady v. Maryland;
- Individuals who have obtained a valid Court Order, subpoena, or otherwise approved in writing by the District Attorney or written designee.

9. Training

SCCDA shall provide staff with a copy of this Surveillance Use Policy when training on the secure handling of confidential and personal information, including data collected by data extraction/examination forensic tools and software. The training shall address appropriate handling and transmission procedures, as well as consequences of misuse of the data and a security breach.

10. Oversight

District Attorney’s Office Administration shall ensure compliance with this Surveillance Use Policy and all applicable laws. When the data extraction/examination forensic tools and software have embedded audit features, the SCCDA Administration shall conduct audits as it deems necessary, and at least annually, to ensure appropriate use of the forensic tools and software.

//

Office of the District Attorney Surveillance Use Policy – Data Extraction/Examination Tools and Software

November 2018
Sanctions for violation of this Surveillance Use Policy or applicable laws may range from counselling to termination, and in more serious breaches, may result in criminal prosecution.

Approved as to Form and Legality

Rob Coelho
Office of the County Counsel