1. General

1.1. Certain precautions need to be taken to preserve potentially volatile evidence residing on electronic devices as they are submitted to the Crime Laboratory for analysis.

1.1.1. The St. Louis County Police Crime Laboratory is located on the 4th Floor of the Police Headquarters Building (7900 Forsyth Blvd, Clayton, MO, 63105).

1.2. Many mobile devices can receive a remote-wipe command that would permanently delete all data on the device. They can also broadcast their location to family/friends of the owner.

1.3. A Digital Forensic Examiner is on-call 24/7 and can be contacted by through the St. Louis County Police Bureau of Communications at 636-529-8210 for consultation or questions.

1.4. This document, and any forms found within can be found at: https://stlouiscountypolice.com/who-we-are/crime-laboratory/

2. Search Authority

2.1. If the owner of the device is alive then a search warrant or signed consent is required for a digital device to be examined.

2.2. Consult with a prosecutor regarding required search authority for a device that is shared with a significant partner or other party.

3. Submission Documents

3.1. Required for each submission are the following;

3.1.1. Evidence Receipt

3.1.2. A copy of the Search Authority

3.1.3. A Submission Form

3.2. Optional Document

3.2.1. Priority Request Form

4. Routers

4.1. Do NOT disconnect from power, reboot, or seize the router. They must be examined in place.

4.2. Disconnecting them from power or rebooting them will often permanently delete the log files needed for the investigation.

4.3. Contact the St. Louis County Bureau of Communications to consult with the On-Call Examiner.

5. DVR / NVR Submissions

5.1. Most Digital Video Recorders (DVRs) or Network Video Recorders (NVRs) can be examined on-scene by receiving consent and working with the owner of the device.

5.2. If login credentials are unknown the device will need to be seized and submitted to the Crime Lab for analysis.

5.3. Ensure both the displayed date/time of the system, as compared with the date/time of a mobile phone, is recorded in the seizing documentation and/or the police report.

6. **Mobile Phones / Tablets**

6.1. The content within a mobile device is highly volatile and how they are handled prior to submission will greatly impact any lab's ability to gain access and extract usable data.

6.2. If the evidentiary device is not isolated from cellular networks, Bluetooth networks, and other mobile devices from the same manufacturer, then the evidentiary device can receive a remote wipe command which will permanently delete the data within or it can broadcast its location to those that have access to the account credentials.

6.3. Turning the device off, or allowing it to reboot, will securely lock all unencrypted data and may permanently prevent access to the data on the device without the passcode.

6.3.1. Turning on Airplane Mode will, at the time of the release of this policy, effectively isolate an Android device and will prevent an Apple device from authenticating a remote wipe command. However, merely swiping down from the top of the screen might only place an Apple device in Airplane Mode for 24 hours, at which time it will revert back to being vulnerable.

6.3.2. A high quality Faraday Bag will isolate the device from all cellular, WiFi, and Bluetooth Networks. However, the device's battery will drain much faster while inside the faraday bag because it is working harder to find a signal. For this reason, a portable charger will need to be connected to the device and packed inside the faraday bag.

6.4. **<u>If The Device is OFF</u>**

6.4.1. **LEAVE IT OFF!**

6.4.2. Package each device as evidence in its own envelope and submit it to the St. Louis County Police Crime Lab for analysis.

6.5. **<u>If The Device is ON</u>**

6.5.1. **LEAVE IT ON!**

6.5.2. Submit each device packaged individually to the St. Louis County Police Crime Lab as soon as possible and transfer it to the Blocker Locker located in the lobby of the Crime Lab. Instructions are in Section 10 below.

6.5.3. After-hours access to the Crime Laboratory for Non-St. Louis County Staff can be obtained by contacting the St. Louis County Bureau of Communications and requesting a security officer provide an escort.

6.5.4. The device, once in the lobby of the Crime Lab, cannot be transferred from one faraday bag to another – including the Blocker Locker faraday bags. Doing so would negate the steps taken by using a faraday bag.

6.5.4.1. If the device is already in a faraday bag (with a power bank) bring the evidence to the Evidence Reception Counter of the Crime Lab, during business hours, and request a Digital Forensics Examiner to assist in safely removing the mobile device from the faraday bag.

7. **<u>Computers</u>**

7.1. If the desktop computer, laptop computer, or any peripheral devices are off, keep them off. Photograph the devices and seize them with their power cables. Do not seize the mouse, keyboard, or any monitors.

7.2. If the desktop or laptop computer is on contact the St. Louis County Bureau of Communications to consult with the On-Call Examiner.

7.3. Have everything photographed while also photographing the area around the devices looking for passwords or encryption keys that will appear as a line of text, numbers, or random words.

8. **<u>Digital Cameras, USB Drives, or other Computer/Camera Drives</u>**

8.1. Package and seize as evidence (with power cables)

9. **Skimmers / GPS Trackers / Smart Assistants**

9.1. Package and seize as evidence (with any associated parts, cabling, or objects found nearby)

10. Blocker Locker Submissions

10.1. The faraday bags inside the Blocker Locker are designed to block cellular, Wi-Fi, and Bluetooth signals while also providing power to a mobile device.

10.2. Instructional videos for how to place a device inside the Blocker Locker's faraday bags are available here or by scanning the QR code next to the Blocker Locker. Otherwise, complete the following steps;

10.2.1. Select an empty bay – indicated by the key still present or request a key from the Crime Lab Evidence Reception staff.

10.2.2. Remove the faraday bag from the bay.

10.2.3. Select the appropriate charging cable from the outer pocket of the faraday bag.

10.2.4. Place the mobile device inside the faraday bag and connect the charging cable to both the device and the charging cable inside the faraday bag.

10.2.5. Roll down and snap the top of the faraday bag.

10.2.6. Place the faraday bag back inside the bay ensuring that it is connected to the charging cable inside the bay.

10.2.7. Place the following inside the bay but **not** inside the faraday bag.

10.2.7.1. An empty, filled-out evidence envelope.

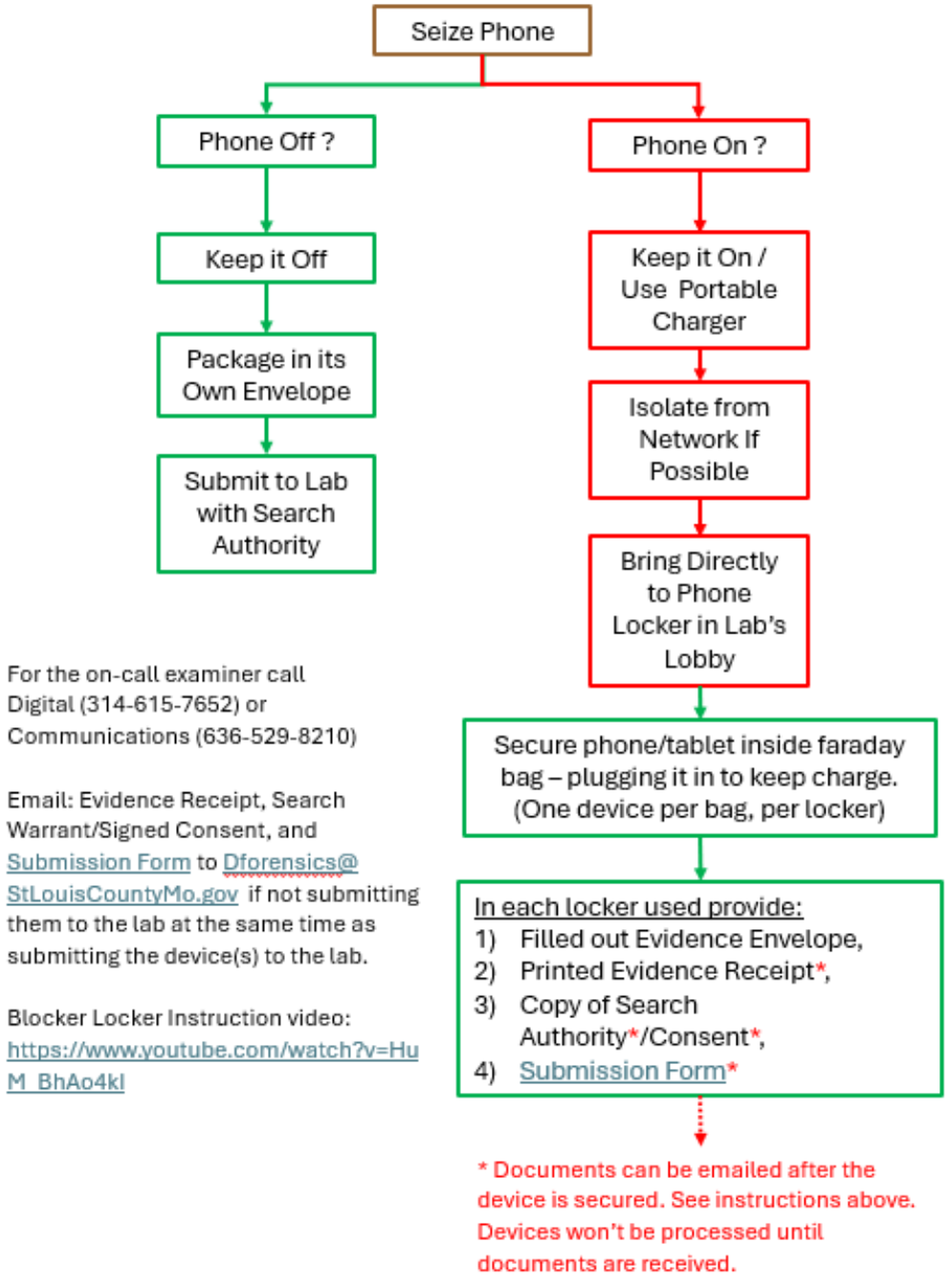
10.2.7.2. An original St. Louis County Police Evidence Receipt or CARE receipt.

10.2.7.3. A copy of the search warrant or signed consent.

10.2.7.4. A completed copy of the Digital Submission Form.

10.2.8. Lock the bay and drop the key in the slot on the left side of the Blocker Locker.

Submitting Phones/Tablets to Crime Lab



For the on-call examiner call Digital (314-615-7652) or Communications (636-529-8210)

Email: Evidence Receipt, Search Warrant/Signed Consent, and Submission Form to Dforensics@StLouisCountyMo.gov if not submitting them to the lab at the same time as submitting the device(s) to the lab.

Blocker Locker Instruction video: https://www.youtube.com/watch?v=HuM_BhAo4kI

For additional information/instructions, see Crime Lab's Website at: https://stlouiscountypolice.com/who-we-are/crime-laboratory/digital-forensics/

January 15, 2025