SILVER BAY POLICE DEPARTMENT
FORENSIC COMPUTER EXAMINATION AND EXTRACTION POLICY

POLICY #D-17

I. PURPOSE

The purpose of this policy is to establish uniform guidelines, which Silver Bay Police Officers shall follow for the handling and examination of mobile devices or other devices capable of or utilized for storing digital data.

II. POLICY

It is the policy of the Silver Bay Police Department to establish guidelines and procedures for the proper handling of mobile devices, and all other devices used or capable of storing digital data, which are submitted for examination to a forensic examiner.

The primary functions for conducting a forensic examination or extraction of data from a mobile device or from other devices capable or utilized for storing digital data are:

1. to acquire the evidence without altering or damaging the original device or data.
2. to authenticate that the acquired evidence is the same as the originally seized data.
3. to analyze the evidence, without modifying.

III. DEFINITIONS

A. Digital Evidence: Digital evidence is a broad term for any data included on a mobile device or on other devices capable of or utilized for storing digital data, which are taken into the custody by a peace officer of the Silver Bay Police Department.

B. Mobile Device: A piece of portable electronic equipment that may connect to the internet, is capable of sending, receiving or storing multiple forms of data, which may include, but is not limited to, contact information (names, aliases, phone numbers, addresses, email addresses, etc.), messages (sms and mms text messages), voicemails, calendars, photographs, videos, audio files, internet browsing activity and cache, and GPS related information.

C. Other Devices Capable or Utilized for Storing Digital Data: A portable storage device which may include, but is not limited to, SD cards, thumb drives (jump drives, flash drive), memory sticks (SIM Cards) and other like devices.

D. Forensic Examiner: A licensed peace officer of the Silver Bay Police Department assigned to the digital forensic lab and certified as a digital forensic examiner.

E. Supervisor: The Chief of Police and/or Sergeant for the Silver Bay Police Department.

F. Proper Authority: A lawful reason that is typically granted by a search warrant, owner consent, exigent circumstances, and other legal means.

G. Examination Types:

1. Logical Examination: An examination that will cover just the file system, as it exists on the mobile device, and is usually limited to just the data that would be available to the user of the device, but in some cases may contain deleted content.

2. Physical Examination: An examination that recovers images of the entire mobile device's memory and may allow for the recovery of deleted content.

3. Manual Examination: An examination which is used when other means to recover data are not available. This examination requires the forensic examiner to manually manipulate the mobile device, while using the mobile device's screen and operating interface. The taking of screen shots will also be necessary to document evidentiary items. This type of examination is commonly conducted by the investigating officer.

4. File System: An examination which acquires files present in or on the mobile device's memory, including images, videos, database files, system files, logs and other like information. These examinations may acquire deleted information when allocated in databases and other files, and may include hidden (protected) files.

H. Network Attached Storage (NAS): A dedicated external file storage system.

I. Child Sexual Abuse Material (CSAM): Any visual depiction of sexually explicit conduct involving a minor (a person less than 18 years of age).

IV. DESIGNATED FORENSIC AREA

A. LAB ACCESS AND RULES

1. Only forensic examiners will be given access to the lab by use of a key fob.

2. At no time will any forensic examiner share their credentials and/or key fob or allow anyone to use them.

3. All visitors to the lab acting in the official capacity must be accompanied by a forensic examiner.

4. Defense attorneys and defense experts will not be allowed access to the lab without prior authorization from the County Attorney and forensic examiner.

5. Maintenance and cleaning personnel will not enter the lab unless escorted by a forensic examiner.

6. Personal or work-issued mobile devices, except those subject to examination, will not be allowed in the lab.

B. DESIGNATED COMPUTER USAGE AND RULES

1. Forensic examiners will be given administrative rights to the lab computer to perform system modifications, such as installing software or changing network settings, and to create, delete, and modify items and settings.

2. Having internet available is helpful to resolve locations in extracted data and update virus definitions easier. It is recommended that the forensic examiner disconnect the internet during the examination until it has been saved to the Network-Attached-Storage (NAS) and removed from the computer's primary data storage. Once the examination has been saved to the NAS, the internet shall be reconnected for weekly scheduled updates via remote access by Lake County Information Systems. The NAS will only be accessible from the lab computer when it has been disconnected from the internet.

3. The lab computer will be used only for official law enforcement purposes and shall be kept in the forensic lab and only be removed with authorization of the CLEO or his/her designee.

C. DESIGNATED LAPTOP COMPUTER

1. A designated laptop computer with no access to the internet will also be made available to the forensic examiner and any licensed peace officer assisting in

the lab. The designated laptop computer shall be kept in the forensic lab and only removed with authorization of the CLEO or his/her designee.

V. PROCEDURES

A. EVIDENCE INTAKE

1. Prior to receiving any mobile device and/or other devices capable or utilized for storing digital data, a "Lab Request For Service" form shall be fully completed and turned into a licensed peace officer and/or evidence technician of the Silver Bay Police Department.

2. All mobile devices and/or other devices capable or utilized for storing digital data accepted by a licensed peace officer and/or evidence technician of the Silver Bay Police Department, shall be properly received, stored, and entered as evidence into the Silver Bay Police Departments records management system and in compliance with Silver Bay Police Department Policy #D-9 (Property and Evidence Policy).

3. The forensic examiner will ensure that proper authority exists for the examination of all mobile devices and/or other devices capable or utilized for storing digital data. The forensic examiner shall ensure a copy of the proper authority related paperwork from the requesting licensed peace officer is received.

B. PRIOR TO STARTING AN EXAMINATION

1. Upon receipt of evidence from the Property and Evidence Storage Room and/or Other Designated Storage Area, or from a licensed peace officer and/or the evidence technician of the Two Harbors Police Department, the forensic examiner shall document how the evidence was packaged upon receipt, and shall include such documentation within the appropriate written report of the forensic examiner.

2. The forensic examiner upon removing the evidence from its packaging shall ensure the mobile device and/or other devices capable or utilized for storing digital data are in the proper "mode" required to conduct the examinations.

3. The forensic examiner shall then take photographs of the evidence, which will document the overall condition and state of the evidence, and if possible, provide the make, model, serial number, and all other identifying information of the evidence being examined.

4. The forensic examiner shall then create a “folder” in the designated computer’s primary data storage area. Only the forensic examiner assigned to this investigation shall have access to the “folder”.

5. The forensic examiner shall then enter the appropriate device description, case number, evidence number, along with the badge number and initials of the examiner into the folder and log.

C. EXAMINATION

1. The forensic examiner shall then determine which type or types of examination(s) are needed and necessary on a case-by-case basis, all while considering the nature and type of investigation being conducted.

2. Upon completion of all necessary and needed examinations, the forensic examiner shall save the results of the examination to the NAS device, and a working copy may be given to the requesting licensed peace officer or their designee. The results of examinations for outside agencies will not be saved to the NAS.

D. POST EXAMINATION OF EVIDENCE

1. The forensic examiner shall then remove the results of the examination from the main dedicated computer primary data storage area, within one (1) working day.

2. The forensic examiner shall then return all evidence to the proper storage location at the Silver Bay Police Department. In the event the evidence examined came from an outside agency, the items of evidence shall be returned to the licensed peace officer, or their designee and chain of custody shall be documented.

3. The forensic examiner shall then complete a detailed and accurate report, which documents receipt and condition of evidence, description of photographs taken, details of the examination process and overall and general details of the findings of the examination. This written documentation shall be in addition to any reports generated by the examination equipment.

4. In the event that CSAM is suspected or found by the forensic examiner, they will contact the requesting investigator as soon as possible and will notify them of the suspected CSAM.

E. CASES INVOLVING CHILD SEXUAL ABUSE MATERIAL (CSAM)

1. CSAM images can only be released to law enforcement investigators directly involved in the investigation, the prosecutor, and the National Center for Missing and Exploited Children's Child Victim Identification Program.

2. The forensic examiner and anyone taking possession of evidence that is known to contain CSAM will follow proper chain of custody protocol.

3. If evidence is to be released and the person requesting release doesn't meet the requirements of Section E, subd. 1, the CD will NOT contain the CSAM images.

4. When extraction materials are wanting to be analyzed and/or viewed and suspected or known CSAM images exist, the dedicated laptop located in the designated office space of the forensic lab shall be utilized for analysis and/or viewing.

F. AUDIT, CHECKS AND BALANCES

1. The supervisor will have the authority to deny requests for data extractions of devices, including but not limited to requests from other agencies, internal complaints, critical incidents, and other large-scale investigations.

2. The supervisor will have the authority to request an audit of the key fob entrance, conduct an audit of use of the computer, and examine the log book.

G. TRAINING & EXAMINATION DOCUMENTATION

1. The supervisor may approve the forensic examiner to conduct training exercises using forensic examination equipment and lab computer. The purpose of this training is to stay current on forensic technology, extraction techniques, and to show other sworn LEO's examples of the capabilities and limitations of this equipment. Forensic examiners shall be responsible for documenting and ensuring the security of the forensic lab and the contents of it including the forensic examination equipment and all other equipment related to the forensic lab.

2. The forensic examiner shall keep a log of all extractions they conducted, assisted in or were present for.

VII. SUPERVISORS SIGNATURES

_____	_____
Cole W. Ernest Chief of Police	Sergeant

VII. EFFECTIVE DATE:

VIII. REVISED DATE: