IN THE {courtTypeUpper} COURT OF LANCASTER COUNTY, NEBRASKA

|  |  |  |
| --- | --- | --- |
| **STATE OF NEBRASKA**  **COUNTY OF LANCASTER** | **)**  **) ss.**  **)** | **AFFIDAVIT FOR SEARCH WARRANT** |

{userName}, a certified law enforcement officer for the {agencyType}, being first duly sworn upon oath deposes and states that Affiant is currently involved in the investigation of {crimeName}, {statuteName}, occurring in {crimeLocation}, Nebraska.

**Affiant’s Background**

Affiant has been a law enforcement officer since {commissionYear}. Affiant has received basic academy training and additional training through the {trainingAgency}. Affiant has experience in conducting criminal investigations including misdemeanor and felony offenses. {additionalTraining}

This Affidavit is being submitted for the limited purpose of securing a search warrant. Affiant has not set forth every fact known regarding this investigation. The facts contained in this Affidavit are based in part on the investigation that Affiant has conducted or information provided to Affiant by other law enforcement officers.

**Case Facts**

{caseFacts}

**Technical Information Regarding the Search of Digital Devices**

Through Affiant’s training and past experience, and from information provided by Electronic Evidence Unit forensic examiners, Affiant is aware that:

Digital devices are often used to communicate via voice, text messaging, social media or other communication applications; and share data with other users and that such digital data can be transferred between various digital devices. Information associated with such data may show evidence of past, current, and future criminal activity. The information also assists law enforcement in determining the identity and culpability of participants, and the identity of victims and/or witnesses. As such, digital devices can serve both as an instrument for committing crime, as well as a storage medium for evidence of the crime.

There have been numerous instances where criminal participants utilized digital devices to photograph themselves, associates and/or co-conspirators, and victims; instances in which digital devices were used by criminal participants to create videos of their criminal activity; instances where criminal participants have used digital devices’ internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within digital devices; and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators and/or a victim.

On a digital device, data can be created in a matter of moments because most operations can be performed almost instantly, which would be relevant to the crime(s) being investigated. The data can be created intentionally or accidentally by the user, or automatically by the digital device itself as a part of its regular functioning. Through the normal operation of a digital device, it logs location data, user interactions, passwords, keychains, notifications, wireless connections and stores this information in databases and/or file systems.

Electronic evidence (data) can remain on the digital devices for indefinite periods of time after the data was created, even if deleted by the user. Data generally is stored on the physical memory of the digital device, but also can be stored on removable storage devices, such as Secure Digital (SD) and Subscriber Identification Module (SIM) cards. A forensic examiner may be able to recover information deleted by the user throughout the working life span of the device.

The following are examples of how types of data on digital devices can assist law enforcement. A full, all-inclusive list would be difficult due to the ever-increasing development of types of data, digital devices and their applications:

1. Digital device information, configurations, calendar events, notes and user account information which can be used to identify or confirm who owns or was using a digital device. Digital devices are commonly small size and can easily be passed from one person. As such, it is necessary to document evidence that reveals or suggests who possessed or used the device.
2. Communication records can establish familiarity between criminal participants, witnesses, and/or victims involved in the crime(s). These records are consistently stamped with dates and times, which can assist in the reconstruction of the timeline of events regarding the investigation. Associated contact lists stored in the device can provide names to correspond with voice calls as well as other forms of communication. Voicemails can indicate the purpose of the phone call when the phone call was not answered. This information can also be invaluable to establish criminal participants and/or co-conspirators, witnesses, and/or details of the crime.
3. Data from associated supplemental software applications (apps), both standard and manually installed, stored on the digital devices can demonstrate the user’s association with other criminal participants or co-co-conspirators, witnesses, and/or victims; crime scenes or other locations; crimes and/or events leading up to or after the crime has been committed. Digital devices can run apps which allow them to increase their functionality. Common programs include social media applications, such as Facebook, as well as messaging applications, such as Snapchat and Facebook Messenger to name a few. These applications are increasingly used as alternative methods for users to communicate from the standard messaging service as they offer additional functionality. Many of these applications can determine the user’s geographic location, which can be instrumental to completing an investigation.
4. Media files such as images, videos, audio, and documents provide first-hand documentation of actions regarding an event. Additionally, files can contain embedded metadata that show additional information which is valuable to investigators such as when and where the file was created. Digital devices can create, store, and exchange media with other devices and computers, including downloading documents from outside sources.
5. Digital devices often generate location data that is shared with the applications or services on the device. Location data can assist law enforcement as to the whereabouts of the device prior to, during, and after the crime took place.
6. Digital devices operate wirelessly and have capabilities to connect through various means, such as a Wi-Fi connection, Bluetooth connection, or cellular network. Each of these connections utilize a different address(es) or name(s), depending on the technology; and these connections are recorded by the digital device.
7. Financial data is also maintained by digital devices through applications or the device itself. Digital devices have the capability to complete financial transactions and store financial information.

As explained herein, information stored in digital devices may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation. In Affiant’s training and experience, digital device data can indicate who has used or controlled the digital device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

To obtain and search the data from the aforementioned digital device, Affiant may need to enlist the aid of non-law enforcement who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. Further, Affiant or those assisting will use the most reasonable means necessary to analyze the data; but, it may be necessary to repair or replace components, or utilize potentially destructive methods. Affiant requests authorization to utilize any means necessary to obtain and analyze the requested data.

The search of digital devices is a lengthy process requiring special steps to ensure the integrity of the digital devices. In the event the search and/or seizure of evidence is not completed within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days upon completion of the search and seizure.

{additionalTechnicalInfo}

**Property to be Searched and Seized**

Affiant requests to search the following device(s) in the possession of the Lincoln Police Department, Lancaster County, Nebraska, including any digital storage device within:

{deviceDescription} labeled with Property Number {propertyNumber}  
   
Specifically for the following items within the time frame of {startDate} at {startTime} {timeZone} to {endDate} at {endTime} {timeZone}:

{evidenceSoughtList}

The search of digital devices is a lengthy process requiring special steps to ensure the integrity of the digital devices. In the event the search and/or seizure of evidence is not completed within ten (10) days, Affiant is requesting authorization to return the search warrant within ten (10) days upon completion of the search and seizure.

Further Affiant sayeth not.

Dated this \_\_\_ day of August, 2025.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{userName}, Affiant

SUBSCRIBED to in my presence and sworn to before me this ­­­\_\_\_ day of August, 2025.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge of the {courtType} Court

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name of Judge

IN THE {courtTypeUpper} COURT OF LANCASTER COUNTY, NEBRASKA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **STATE OF NEBRASKA**  **COUNTY OF LANCASTER** | **)**  **) ss.**  **)** | **SEARCH WARRANT** | |  |

TO: {userName}, a certified law enforcement officer with the {agencyType}, Lancaster County, Nebraska, any and all law enforcement officers, or others as needed by law enforcement.

WHEREAS, {userName} has filed an Affidavit before the undersigned Judge of the {courtType} Court of Lancaster County, Nebraska, and said written Affidavit, having been duly considered, the court finds that the facts set forth in said Affidavit are true, and that those facts do constitute grounds and probable cause for the issuance of a Search Warrant pursuant to Neb. Rev. Stat. § 29-814.04.

THEREFORE, you are commanded to search and seize the items as described below.

**Property to be Searched and Seized**

Law enforcement, and those assisting law enforcement, is directed to search the following device(s) in the possession of the Lincoln Police Department, Lancaster County, Nebraska, including any digital storage device within:

{deviceDescription} labeled with Property Number {propertyNumber}  
   
Specifically for the following items within the time frame of {startDate} at {startTime} {timeZone} to {endDate} at {endTime} {timeZone}:

{evidenceSoughtList}

Furthermore, the Court finds that law enforcement may use any means reasonably necessary to access and seize the above mentioned items.

This Search Warrant shall be executed and returned within ten (10) days to the undersigned Judge of the {courtType} Court of Lancaster County, Nebraska. In the event the search and/or seizure is not complete within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days upon completion of the search and seizure.

Given under my hand and seal this \_\_\_ day of August, 2025.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge of the {courtType} Court

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name of Judge