	STANDARD OPERATING PROCEDURE State Form 39870 (R/ S- 06)	Reference Number INV-026
	Subject Seizure of Cryptocurrency and Virtual Assets	
	Special Instructions Replaces INV-026 dated May 15, 2018	Effective Date **December 10, 2025**

I. PURPOSE

The purpose of this policy is to provide Indiana State Police officers with guidelines for the seizure of cryptocurrencies and virtual assets.

II. POLICY

It is the policy of the Indiana State Police to seize cryptocurrencies and virtual assets in a forensically sound manner. Controls will be used to ensure properly conducted seizures and protect against improperly conducted seizures.

III. DEFINITIONS

A. AGENCY CONTROLLED WALLET – A virtual asset wallet that is controlled by the Indiana State Police either by controlling the private key, seed phrase, or through a virtual asset service provider.

B. BLOCKCHAIN - A digital ledger in which transactions made in a virtual asset or cryptocurrency are recorded chronologically and publicly.

C. COLD STORAGE WALLET - A virtual asset wallet kept offline on a hard disc drive, electronic storage media, a bearer instrument, or in paper hard copy.

D. CRYPTOCURRENCY/VIRTUAL ASSET - A centralized or decentralized medium of exchange, which may be based on an online public ledger and operates like a currency in some environments, but does not have all the attributes of real currency. Examples of virtual assets include, but are not limited to, Bitcoin, Ethereum, XRP, Tether, BNB, and Solana.

E. EXCHANGE/VIRTUAL ASSET SERVICE PROVIDER - A digital marketplace where traders can buy and sell virtual assets using different fiat currencies or other virtual assets.

F. HOT STORAGE WALLET - A virtual asset wallet which is online and connected in some way to the Internet.

G. PRIVATE KEY - A sophisticated form of cryptography which allows a user to access their virtual asset.

H. PUBLIC KEY - a cryptographic code which allows a user to receive virtual asset into their account.

I. RESTORE – Reinstall an operating system or restore to a previous virtual machine snapshot in such a manner to cause data files, program files and metadata from the previous state of the operating system to be inaccessible or unrecoverable.

J. SEED PHRASE – A sequence of 12 to 24 random words that stores the information needed to recover a virtual asset wallet.

K. SEIZING OFFICER - Sworn officer of the Indiana State Police responsible for the seizure of virtual assets. This officer is also responsible for maintaining chain-of-custody when transferring virtual assets between Agency Controlled Wallets and Virtual Asset Service Providers. The Seizing Officer will have sufficient training, knowledge, skills, and abilities to perform the seizure in a forensically sound manner.

L. WALLET - A software program in which one or more private keys or seed phrases are stored, a bearer instrument in which one or more private keys or seed phrases are stored, or a paper hard copy on which one or more private keys or seed phrases are written.

M. WITNESSING OFFICER - Sworn officer of the Indiana State Police responsible for observing the seizure and storage of seized virtual assets. The Witnessing Officer will have sufficient knowledge, skills, and abilities to fully understand the seizure process and safeguards being employed.

IV. PROCEDURE

A. When the virtual asset subject to seizure is in a hot storage wallet located on a virtual asset service provider and the virtual asset service provider will comply with a seizure order issued by judicial authority, such order will be served on the virtual asset service provider by the seizing officer.

1. The seizing officer will generate a new deposit address from an agency controlled wallet for each virtual asset to be seized.

2. The seizing officer will send the deposit addresses for each virtual currency to the compliant virtual asset service provider to have them send the seized virtual assets to the agency controlled wallet.

3. If the agency controlled wallet is unable to accept the virtual asset, the type of virtual asset and amount shall be documented and alternate wallet software may be used with approval of the Captain of Special Investigations.

B. When the virtual asset subject to seizure is either in a hot storage wallet (when the virtual asset service provider will not comply with a seizure order issued by judicial authority), exigency exists such that it is not feasible to serve a seizure order on the virtual asset service provider, the virtual asset is in a cold storage wallet, or when only a seed phrase or private key is located the following seizure process shall be utilized:

1. If utilizing a virtual machine environment for this process, a snapshot of the system should be taken before continuing.

2. The seizing officer will take screen captures, screen record, photograph, or otherwise document throughout the entirety of the process of the virtual asset seizure. These digital captures and documentation shall include the types of asset and initial amounts of virtual assets subject to seizure, the deposit addresses generated, the transaction dates and times of the transfers to the agency controlled wallet, the transaction hashes generated for each transfer, the confirmation on the blockchain (if available) of the transfer, and the confirmation within the agency controlled wallet of the receipt of the seized virtual asset. These processes will be observed at all times by the witnessing officer.

3. The seizing officer will generate a new deposit address from an agency controlled wallet for each virtual asset to be seized.

4. The seizing officer will use the private key or seed phrase for the virtual asset subject to seizure in conjunction with a well-established and verified hot wallet software to transfer the seized virtual asset to the agency controlled wallet.

5. In instances in which more than one private key exists in the same wallet subject to seizure, a new deposit address within the agency controlled wallet will be created for each wallet subject to seizure (e.g. if the same subject has hot storage accounts with different virtual asset service providers, a new deposit address from the agency controlled wallet will be created and used for each wallet subject to seizure.).

6. When possible, the seizing officer will use the respective virtual asset's blockchain to confirm the transfer was successfully accomplished from the wallet subject to seizure to the agency controlled wallet.

7. The seizing officer will copy all screen captures, screen recordings, photographs or other documentation* to storage medium (CD, DVD, USB Drive, Hard Drive). Alternately, if a virtual machine environment was used for this process, the virtual machine file with all recorded contents may be placed on storage medium. This storage medium will be packaged and handled as money in accordance with FSD-005.

NOTE: Due to the nature of the recorded information, no photographs or documentation of the seizure process shall be uploaded to AXON.

8. Both the seizing officer and the witnessing officer will affix their signature, date, time, and other pertinent information to the storage medium following in accordance with FSD-005.

9. The storage medium will be submitted for storage as money in accordance with FSD-005.

10. The computer used to facilitate the seizure shall be restored immediately following the seizure. This restoration may occur by either reinstalling the computer's operating system or by restoring from the previously created snapshot. This process will be observed at all times by the witnessing officer.

11. The seized cryptocurrency will not be converted to United States Currency until a forfeiture order is issued. This is consistent with existing policy and practice when seizing other items

which can fluctuate in value (e.g. precious metals, houses, negotiable instruments, vehicles, works of art, and foreign currencies).

C. When using a virtual asset service provider as an intermediary to the agency controlled wallet only the Virtual Asset Investigations Team lead, the Captain of the Special Investigations Division, and the Major of the Legal / Legislative Affairs shall have access to the account.

D. This procedure is to be used in conjunction with all relevant Department regulations, rules, policies and procedures.