1. Executive Summary

Too many losses are attributable to lost keys. Everyone knows this is solvable. In the post mortem of hacks, the reasons for lost keys are never discussed. This means we do not have the data to improve.

This document will try to change this. We want each protocol to publicly write down the process their signers use to sign transactions that change DeFi protocols. Once a process is in writing, when a key is compromised, the question becomes how? What went wrong? How can the process be improved so this does not happen again? Put this information in the post mortem (sanitized for privacy) and everyone knows how they can improve and all DeFi improves.

For DeFiSafety scoring, only the wallets that affect the DeFi protocol need to follow this process (changing the code or coefficients). These are wallets that affect other people's money. So DAO transactions are not required.

Any policy is better than no policy so our scoring reflect this. Auditing the process, so that DAO members are convinced the process is being followed adds to the score.

1.1 Question

This is the question we intend to ask.

Is there a robust documented transaction signing policy?

Guidance:

80% Robust transaction signing process (7 or more elements) with no audits evident
70% Adequate transaction signing process (5 or more elements) with no audits evident
60% Weak transaction signing process (3 or more elements) with no audits evident
0% No transaction signing process evident

Evidence of audits of signers following the process add 20%

2. List of transaction signing elements

Policies for signers

1) All signers must use one of the following desktop wallets (Metamask, WalletConnect, etc)
2) All signers must use an approved hardware wallet (Trezor, Ledger, etc)
3) All signers must use an approved browser (Brave, Firefox, etc)
4) All transactions must occur on a dedicated browser instance (rather than a dedicated computer).
5) All hardware wallets must be exclusively for access control purposes of this protocol. In other words, the hardware wallet should not be used for personal transactions or development transactions on the protocol.
6) An approved VPN should be used for all transactions.
7) Committed in writing that the backup of keys are in multiple locations and protected from fire and flood
8) All signers on all access control addresses must sign a transaction at least once every X months. This can be an active transaction or a test transaction.
9) All access control transactions must be executed in a controlled space for example home or office. They should not be signed in public spaces such as coffee shops or airport terminals.
10) All access control transactions must be executed through a dedicated computer. This computer is used only for transactions, never e-mail or web browsing. It should use minimal approved communication between computers, for example I only use Telegram.
11) The dedicated computer should not use the same local network as the users main computer to mitigate that computer is compromised and infects the dedicated computer
12) All access control transactions must be executed in a dedicated space using an approved computer. This is an extreme example. The protocol could rent access to a controlled room that requires a key card for access. In this room there is a dedicated computer used for these transactions only.

3. Example Robust Transaction Policy

This document contains the transaction policy for XX protocol. All transactions that affect the deployed code or impact user funds must use this policy. The list of addresses where this policy must be used is in Section 3.2. The signers addresses for each address is listed in Section 3.3.

3.1.Policies for signers of transactions

All signers (listed in section 3.3) of the addresses (listed in section 3.2) must follow this policy:

1) All signers must use the latest version of the Metamask desktop wallets.
2) All signers must use an updated Ledger hardware wallet
3) All signers must use an approved browser (Safari, Chrome or Firefox)
4) All hardware wallets must be exclusively for access control purposes of this protocol. In other words, the hardware wallet should not be used for personal transactions or development transactions on the protocol.
5) All signers have signed a declaration that they have 2 backups of their seed phrase in separate locations that are safe for fire and flood.
6) All signers on all access control addresses must sign a transaction at least once every 3 months. This can be a test transaction to a separate address (not listed in 3.2).
7) All access control transactions must be executed in a controlled space for example home or office. They should not be signed in public spaces such as coffee shops or airport terminals.
8) All access control transactions must be executed through a dedicated computer. This computer is used only for transactions, never e-mail or web browsing.

3.2. List Addresses this policy covers.

This policy is used for all transactions on the following addresses;

1) xXX_Deployer 0xABC123… on Ethereum mainnet
2) xXX_Deployer 0xABC123… on Optimism

3.3. List of Signers this policy covers.

Address 0xABC123… is a Gnosis Safe multisig with 4 of 7 signers.

Signer 1: 0xDEF678…
Signer 2: 0xDEF678…
etc…

3.4. Audit Policy

A trusted person with the protocol and selected by the DAO will have a private video call with each signer once every six months where they demonstrate how they follow the policy. The trusted person will write a report of the audit results that all DAO members can read.

4. Example Adequate Transaction Policy

This document contains the transaction policy for XX protocol. All transactions that affect the deployed code or impact user funds must use this policy. The list of addresses where this policy must be used is in Section 4.2. The signers addresses for each address is listed in Section 4.3.

4.1. Policies for signers of transactions

All signers (listed in section 4.3) of the addresses (listed in section 4.2) must follow this policy:

1) All signers must use the latest version of the Metamask desktop wallets.
2) All signers must use an updated Trezor or Ledger hardware wallet
3) All signers must use an approved browser (Safari, Chrome or Firefox)
4) All hardware wallets must be exclusively for access control purposes of this protocol. In other words, the hardware wallet should not be used for personal transactions or development transactions on the protocol.
5) All signers have signed a declaration that they have 2 backups of their seed phrase in separate locations that are safe for fire and flood.

4.2. List Addresses this policy covers.

This policy is used for all transactions on the following addresses;

3) xXX_Deployer 0xABC123… on Ethereum mainnet
4) xXX_Deployer 0xABC123… on Optimism

4.3. List of Signers this policy covers.

Address 0xABC123... is a Gnosis Safe multisig with 4 of 7 signers.

Signer 1: 0xDEF678...
Signer 2: 0xDEF678...
etc...