TERM PROTOCOL
SIGNER COMPLIANCE POLICY

Last updated: November 13, 2023

I. Introduction

This Multisig Compliance Policy (the "Policy") sets forth required practices and procedures for signers of certain multisig wallets relating to the Term Protocol (the "Protocol").

II. Covered Persons and Addresses

The following individuals are required to follow the Policy:

1. All signers for the Protocol Admin Safe with address 0x73d1C7dc9CEb14660Cf1E9BB29F80ECF9E97D774 (all networks); and

2. All signers for the Protocol DevOps-Proposer Safe with address 0xd5E12854A3Dba99deF295A7635D3Ba16427d2A28 (all networks).

These above individuals are referred to in the Policy as "covered persons" and the above addresses are referred to as "covered addresses." The wallet used by a covered person to sign for a transaction for a covered address is a "signing wallet."

III. Obligations

In connection with signing transactions for covered addresses, all covered persons must:

1. Use the latest version of the MetaMask browser extension with their signing wallet;

2. Use a Ledger hardware wallet with the latest firmware version installed for their signing wallet;

3. Use the latest version of Chrome or Firefox with their signing wallet;

4. Use a hardware wallet that is used exclusively for access control purposes of the Protocol and that is not used for any other purpose, including personal transactions and non-access control transactions;

5. Sign a declaration that they have two (2) backups of the seed phrase for their signing wallet in separate locations that are secure against fire and flood;

6. Sign a transaction (which can be a test transaction) for the covered addresses using their signing wallet at least once every three (3) months;

7. Execute all access control transactions in a controlled, secure space (such as an office) and not in a public space.

In general, regardless of whether something is listed above, a covered person must take steps to ensure the security of their signing wallet, including protecting the wallet's seed phrase against unauthorized access.

IV. Audit

A trusted person designated by Term Foundation will conduct a private interview (either in person or through a video call) with each covered person at least once every twelve (12) months. During the interview, the covered person will discuss how they comply with the obligations set forth in the Policy. The trusted person will write a report of the audit results that will be added to Term Foundation's records.

V. Attestation

All covered persons must attest at least once every twelve (12) months in writing that they have, and will continue to, comply with the requirements of this Policy.

ANNEX A: FORM OF SIGNER ATTESTATION

I, _____, a covered person as defined in the Term Protocol Signer Compliance Policy (the "Policy"), hereby attest:

1. I have reviewed the Policy at least once in the past twelve (12) months and understand my obligations under it.

2. During the past twelve (12) months, I have been, and remain, in compliance with Policy, including the requirement that I store two copies of the seed phrase for my signing wallet in separate locations that are secure against fire and flood.

_____

Name:
Date: