

This version is valid from October 17, 2026. Latest Update: 16 October 2026.

EMBEDDED WALLET POLICY

Crypto-Holdings Platform

This document (hereinafter referred to as the “Policy”) sets out the terms of use of the Crypto-Holdings Platform at the website crypto-holdings.io using the Embedded Wallet, referred to in § 4 of the Terms of Use. The Platform is operated by Axenor Holdings OÜ, a limited liability company with its registered office in Estonia at: Narva mnt 13-27, 10151 Tallinn, Estonia, registered in the Estonian Commercial Register under number 17426720, LEI: 984500513804D9B6D886 (hereinafter referred to as Crypto-Holdings or the Service Provider). The Policy describes the allocation of roles and responsibilities and the reasons why the Service Provider does not provide custody and administration of crypto-assets or transfer services for crypto-assets on behalf of Users.

§ 1. Definitions

Whenever the Policy refers to:

1. Embedded Wallet – it means the Embedded Wallet within the meaning of § 2 of the Terms of Use, that is a wallet provided by a third-party technology provider which allows the User to create and use a blockchain wallet compatible with the Base network without installing external browser extensions or manually managing private keys in the traditional manner;
2. Wallet Provider – it means the third-party technology provider of the Embedded Wallet functionality, currently MetaMask Embedded Wallets / Web3Auth;
3. Private Key – it means the cryptographic key enabling the authorisation of transactions from the Embedded Wallet;
4. Authentication Method – it means the means used by the User to access the Embedded Wallet, that is e-mail login, social login (e.g. Google, Apple, Discord) or Web3 authentication;
5. External Wallet – it means the External Wallet within the meaning of § 2 of the Terms of Use.

§ 2. Nature of the Embedded Wallet

1. The Embedded Wallet is created only at the User’s request and is assigned to the User’s own address on the Base network. Tokens and other crypto-assets are assigned to that address on the Base network.

2. The Platform does not store the User's seed phrase or full Private Keys in a manner enabling independent access to User funds. The Service Provider does not have the technical ability to independently initiate transactions from the User's Embedded Wallet.
3. The use of the Embedded Wallet does not imply the provision by the Service Provider of custodial services, payment services or the storage of digital assets on behalf of the User. Crypto-assets held in the Embedded Wallet are not pooled with the assets of other Users or of the Service Provider.
4. Each transaction from the Embedded Wallet is initiated and authorised by the User using the User's Authentication Method.

§ 3. Role of the Service Provider

1. The Service Provider integrates the Embedded Wallet functionality of the Wallet Provider into the Platform interface.
2. The Service Provider does not:
 - 2.1. provide custody and administration of crypto-assets on behalf of clients within the meaning of Article 3(1)(17) and Article 75 of Regulation (EU) 2023/1114;
 - 2.2. provide transfer services for crypto-assets on behalf of clients within the meaning of Article 3(1)(26) of Regulation (EU) 2023/1114;
 - 2.3. hold Tokens of Users in trust or otherwise hold, control or manage the crypto-assets of Users.
3. The Service Provider may grant Users limited amounts of ETH to cover Base network fees through the GasVault smart contract (0x3c15c4BeA893FEC8277F8d884250A0F0291Bfa18), within the limits set in that smart contract. Such a grant does not mean the custody of User funds and does not give the Service Provider any control over the Embedded Wallet.
4. The use of the Embedded Wallet is optional. The User may use the Platform with an External Wallet, in accordance with § 4 and § 6 of the Terms of Use.

§ 4. Responsibilities of the User

1. The User is solely responsible for the security of the User's account, device and any Authentication Methods used to access the Embedded Wallet.
2. Access to the Embedded Wallet is restored only through the recovery procedures of the Wallet Provider. The Service Provider cannot recover the User's Private Keys or seed phrase.
3. The User should immediately inform the Service Provider in accordance with § 4 of the Terms of Use if the User suspects unauthorised access to the Embedded Wallet or to the Authentication Methods.

4. The Service Provider never requests the User to provide a seed phrase, recovery phrase, Private Key or one-time authentication codes.

§ 5. Portability

1. The User may at any time transfer the crypto-assets held in the Embedded Wallet to another compatible wallet and, where the Wallet Provider's technology makes it possible, export the Private Key.
2. Transfers of CHT Tokens are subject to the transfer fee described in field E.36 of the Whitepaper and in § 5 of the Terms of Use, and to the Base network fee.

§ 6. Suspension or Termination of the Agreement

1. The suspension of services, the blocking of access or the termination of the agreement in accordance with § 12 of the Terms of Use does not give the Service Provider control over the Embedded Wallet. The User retains access to the Embedded Wallet through the Wallet Provider's technology.
2. Before terminating the agreement, the User should transfer the assets to another wallet or, where possible, export the Private Key.
3. Measures applied at the level of the CHT Token in accordance with the Whitepaper and the Withdrawal Procedure apply equally to the Embedded Wallet and to External Wallets and do not constitute custody of the Embedded Wallet.

§ 7. Wallet Provider

1. The Embedded Wallet functionality is provided by the Wallet Provider and may be subject to the Wallet Provider's own terms of service and privacy policies.
2. The Platform does not guarantee the continuous availability of the Wallet Provider's services or compatibility with all blockchain networks, applications or devices. The Service Provider is not liable for the acts or omissions of the Wallet Provider, unless otherwise stipulated by mandatory provisions of law, in accordance with § 10 of the Terms of Use.

§ 8. Regulatory Status

1. Because the Service Provider does not store the User's seed phrase or full Private Keys in a manner enabling independent access to User funds and does not initiate transactions on behalf of Users, the Service Provider does not provide crypto-asset services requiring authorisation under

Article 59 of Regulation (EU) 2023/1114. The Whitepaper states that no crypto-asset service provider is involved in the offer to the public of CHT Tokens.

2. Should the Service Provider in the future provide any custody or administration of crypto-assets on behalf of Users within the meaning of Article 75 of Regulation (EU) 2023/1114, it shall do so only after obtaining the authorisation required under Article 59 of that Regulation, in accordance with § 6 of the Terms of Use.

§ 9. Final Provisions

1. In matters relating to the User's use of the Embedded Wallet functionality, the provisions of the Policy prevail over the Terms of Use, in accordance with § 11 of the Terms of Use, subject to mandatory provisions of law.

2. The risks related to wallets and private keys are described in § 9 of the Terms of Use and in Part I of the Whitepaper.

3. Information on the processing of personal data shall be found in the Privacy Policy published on the Platform and in the privacy policies of the Wallet Provider.

4. Complaints are submitted and processed in accordance with the Complaints-handling Procedure.

5. The Policy is amended in accordance with § 13 of the Terms of Use. The governing law and jurisdiction are determined in accordance with § 14 of the Terms of Use.