Acceptable use policy

Version 1.0

Reading copy. The authoritative text is the plain-text file whose fingerprint appears below; it is downloadable at the same address with the .txt extension.

SHA-256 fingerprint of the authoritative text : 897e27a4f522dc916586215e4433f894c504459addd2a4dc9a7b56739f95ea40

1. Purpose

This policy defines the prohibited uses of CowriePay. It forms an integral part of the Terms and conditions (www.cowriepay.io/legal/terms) and binds the Client as well as the users it authorises.

These restrictions are not a judgement on any activity. They follow from the law, from our anti-money-laundering and counter-terrorist-financing due-diligence obligations, and from the requirements of the infrastructure the service relies on.

The lists below are indicative and not exhaustive: an activity that does not appear but presents the same risks is treated the same way.

CowriePay is operated by COWRIEX, a Societe par Actions Simplifiee (SAS) registered with the Trade and Personal Property Credit Register of Abomey-Calavi under number RB/ABC/25 B 10127. Full details appear in the Legal notice (www.cowriepay.io/legal/legal-notice).

2. Prohibited users

The service may not be opened or used by:

- any individual or entity appearing on an applicable sanctions list, and any entity owned or controlled by such a person;
- any person acting, directly or indirectly, on behalf of a person referred to above;
- any person established, resident or operating from a country or territory subject to comprehensive restrictive measures;
- any person who refuses to provide the information and supporting documents needed for verification, or who provides inaccurate information;
- any person whose account was previously closed for breach of this policy.

3. Prohibited activities

CowriePay may not be used, directly or indirectly, for:

- money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction;
- circumventing international sanctions, restrictive measures or export controls;
- fraud, scams, phishing, identity theft or any form of deception aimed at obtaining funds;
- extortion, distribution of malware or the collection of ransoms;
- asset-mixing services and, more generally, any arrangement designed to break the traceability of the origin of funds;
- clandestine marketplaces and the sale of unlawful goods or services;
- trade in narcotics, weapons, ammunition or controlled dual-use goods;
- human exploitation, trafficking, and the production or distribution of child sexual abuse material;

- pyramid schemes, Ponzi arrangements and any offer promising a guaranteed return;
- market manipulation and fictitious transactions intended to create the appearance of activity;
- gambling and betting carried on without the authorisation required in the relevant jurisdictions;
- the provision of financial services for which a licence is required, where the Client does not hold one;
- counterfeiting and any infringement of third-party intellectual property rights;
- collecting or holding funds on behalf of third parties outside the framework set out in article 5.

4. Activities requiring prior approval

The following activities are not prohibited but require our prior written approval following enhanced review. Carrying them on without that approval is a breach:

- duly authorised gambling and betting;
- money transfer services, bureaux de change and similar licensed activities;
- digital-asset exchange or custody platforms;
- marketplaces and any activity involving the collection and onward payment of funds to third parties;
- lawful adult content;
- trade in precious metals, precious stones and high-value goods;
- non-profit organisations raising funds internationally.

5. Client obligations towards its own customers

Where the Client uses CowriePay to serve its own customers, it must:

- verify the identity of its end customers in accordance with the regulation applicable to it;
- not give access to the service, directly or indirectly, to unverified third parties;
- not aggregate funds belonging to unidentified third parties in a single account;
- respond to our requests for information within a reasonable time, including on the origin of funds and the identity of beneficiaries;
- inform its end customers of the processing of their data, as set out in the Privacy policy (www.cowriepay.io/legal/privacy).

6. Technical abuse

It is also prohibited to:

- circumvent or attempt to circumvent rate limits, caps, withdrawal controls or any other security mechanism;
- reverse engineer the service, or conduct penetration testing without our prior written authorisation;
- resell, sublicense or otherwise make access to the service available to third parties outside the contractual framework;
- create multiple accounts in order to circumvent a refusal, suspension or closure decision;
- use the Sandbox environment for anything other than testing and integration.

7. Consequences of a breach

Depending on the seriousness and on the obligations incumbent on us, we may:

- open an enhanced review and request further information or supporting documents;
- refuse, hold or delay a transaction;
- suspend all or part of access to the service;
- terminate the contract and close the account;
- freeze assets and, where the law so requires, block them and make the required reports to the competent authorities.

Where the law prohibits us from informing a person of a report or a measure concerning them, we comply with that prohibition.

8. Reporting

If you become aware of any use of CowriePay contrary to this policy, report it to legal@cowriepay.io. For a security incident or a phishing attempt, write to support@cowriepay.io.

9. Changes

We may amend this policy to reflect changes in risks, fraud typologies and the applicable framework. Amendments take effect on publication on this page; in the event of a substantial change we inform the Client by email or in the dashboard.