



Cryptosmart S.p.A.

**Descrizione sintetica del contenuto della Policy relativa alla prestazione di custodia e amministrazione di
cripto-attività per conto dei Clienti**

1. Disposizioni generali

Il presente documento sintetizza il contenuto della *policy* (la “**Policy**”) adottata da Cryptosmart S.p.A. (“**Cryptosmart**” o la “**Società**”) in materia di custodia e amministrazione di cripto-attività per conto dei clienti, ai sensi del Regolamento (UE) 2023/1114 (“**MiCAR**”), con particolare riferimento all’articolo 75 e alle disposizioni applicabili. La Policy rappresenta lo strumento con cui la Società assicura la corretta, sicura e trasparente prestazione del servizio nei confronti dei propri utenti.

2. Finalità e principi generali

Lo scopo della Policy è quello di definire un quadro tecnico-organizzativo volto a garantire la sicurezza, la segregazione e la piena titolarità delle cripto-attività affidate dai clienti, assicurando nel contempo l’aderenza ai requisiti normativi europei. Essa regola i rapporti tra la Società, in qualità di prestatore di servizi di custodia, e ciascun cliente, precisando le modalità con cui sono gestiti i *wallet*, le chiavi private, i fondi correlati e l’esecuzione delle istruzioni trasmesse dal cliente.

3. Natura del servizio e asset custoditi

Cryptosmart fornisce un servizio di custodia che consiste nella detenzione, per conto dei clienti, delle cripto-attività e dei relativi mezzi di accesso (in particolare le chiavi crittografiche private), permettendo altresì l’amministrazione delle stesse sulla base delle istruzioni impartite dagli utenti. Le cripto-attività interessate comprendono sia quelle con emittente identificabile che quelle decentralizzate (ad es. bitcoin).

La Società non detiene direttamente le cripto-attività, bensì conserva e protegge le chiavi necessarie per il loro accesso e utilizzo. La gestione avviene attraverso una combinazione di *hot wallet* e *cold wallet*, tutti in forma *omnibus*. I primi, connessi a internet, sono destinati all’operatività giornaliera; i secondi, *offline*, sono utilizzati per la custodia a lungo termine.

4. Sicurezza e gestione dei wallet

La Società adotta *standard* elevati di sicurezza informatica. I *cold wallet* utilizzano una struttura *multisignature* (3 firme su 6) e prevedono *backup* fisici conservati in cassette di sicurezza presso istituti bancari autorizzati. L’apposizione delle firme può avvenire sia tramite postazioni dedicate *offline*, sia tramite dispositivi mobili dedicati mantenuti *offline* mediante scambio di QR code, garantendo l’assenza di connessioni di rete tra ambiente *offline* e *online*. In caso di dismissione di uno dei firmatari, la Società provvede alla sostituzione delle chiavi e al trasferimento degli *asset* entro cinque giorni lavorativi.

Gli *hot wallet*, invece, sono gestiti mediante tecnologia HD wallet secondo gli standard BIP32/BIP44, e per alcune cripto-attività tramite la piattaforma Fireblocks, con protezione crittografica e controllo distribuito. Il sistema consente la generazione di indirizzi univoci per ciascun cliente e prevede anche il *backup* delle chiavi tramite Bitwarden, con autenticazione multi-fattore e accesso di emergenza.

È previsto un meccanismo automatico che, superate certe soglie, trasferisce le cripto-attività in eccesso dagli *hot wallet* ai *cold wallet* (“MoveFundsFromHotToColdWallet”), limitando i rischi legati alla permanenza di *asset* online.

5. Tracciabilità, riconciliazione e segregazione

Tutte le cripto-attività e i fondi dei clienti sono registrati in *database* dedicati e soggetti a riconciliazioni quotidiane, con verifica dell’equivalenza tra le posizioni individuali e le giacenze effettive.

La segregazione è garantita sia operativamente che giuridicamente: gli *asset* dei Clienti non sono mai confusi con quelli della Società, non rientrano nel patrimonio fallimentare della stessa e sono esclusi da azioni esecutive di terzi. La Policy prevede inoltre il divieto di utilizzo non autorizzato delle cripto-attività dei clienti.

6. Gestione dei depositi e dei fondi fiat

I clienti possono depositare cripto-attività tramite indirizzi dedicati. Il sistema informatico BlockSync monitora costantemente la *blockchain* e, dopo un numero minimo di conferme, registra il deposito e aggiorna il profilo del cliente.

I fondi (es. euro derivanti dalla vendita di cripto-attività) sono depositati su conti correnti segregati intestati alla clientela presso Intesa San Paolo S.p.A., Credito Emiliano S.p.A. e Poste Italiane S.p.A. Il processo di gestione include un meccanismo di firma che coinvolge quattro soggetti apicali interni (due disponenti di pagamento e due firmatari dei conti) e rigorosi controlli di riconciliazione giornalieri.

7. Staking

La Policy disciplina anche la custodia delle cripto-attività impiegate nei servizi di *staking*, con modalità differenziate per Ethereum (uso di “*withdrawal credentials*”), Cardano e Polkadot (*wallet* separati, approvazione *multisig* e selezione dei validatori secondo criteri oggettivi quali basse commissioni, *self stake* e *reward points*). Per Polkadot, la selezione dei nodi validatori richiede una specifica ratifica *offline* mediante firma di almeno tre soggetti autorizzati.

8. Sicurezza informatica e conformità normativa

La Società adotta un framework di sicurezza conforme al Regolamento DORA, comprensivo di:

- crittografia dei dati in transito e a riposo;
- monitoraggio antifrode e *logging* avanzato;
- piani di continuità e *disaster recovery*;
- *audit* regolari e *test* di vulnerabilità;
- autenticazione a tre fattori per le operazioni di prelievo (login, codice e-mail e OTP tramite Google Authenticator).
- formazione continua del personale.

L’infrastruttura *cloud* utilizzata (es. Vultr, Digital Ocean) è ridondata e conforme ai migliori *standard* di sicurezza.

9. Accesso alle informazioni, trasparenza e rendicontazione

La Società garantisce ai clienti accesso continuo ai saldi e movimenti tramite area riservata, con possibilità di esportare il rendiconto. Sono inoltre previsti sistemi di notifica, comunicazioni tempestive in caso di eventi straordinari e la fornitura di informazioni precontrattuali in forma chiara e comprensibile.

10. Responsabilità e tutela del Cliente

La Società risponde verso i clienti in caso di perdita imputabile a proprie omissioni o negligenze, con risarcimento limitato al valore di mercato al momento dell’evento. Sono escluse le responsabilità per eventi di forza maggiore (e.g. attacchi alla *blockchain*, guerre, calamità) o non riconducibili al controllo della Società. In caso di eventi straordinari, la Società si impegna a fornire tempestiva documentazione giustificativa dell’estraneità ai fatti.

11. Diritto di disposizione

Il Cliente ha diritto a disporre in ogni momento delle cripto-attività e dei fondi custoditi, fatti salvi i controlli di sicurezza e antiriciclaggio. Le istruzioni vengono eseguite entro il giorno lavorativo successivo, nei limiti dei tempi tecnici degli intermediari.

12. Revisione periodica e accessibilità

La Policy è approvata dal Consiglio di Amministrazione ed è soggetta a revisione annuale oppure in occasione di mutamenti normativi rilevanti o modifiche sostanziali al modello del Servizio. Una sintesi è pubblicata sul sito della Società e disponibile su richiesta in formato accessibile. La Policy è inoltre resa disponibile alle Autorità di Vigilanza competenti per eventuale esame ai sensi degli articoli 62 e seguenti del MiCAR.