Kriptoturto saugojimas ir administravimas

Šioje Decentralized, UAB (toliau – **Bendrovė**) Kriptoturto saugojimo politikoje, parengtoje pagal Europos Sąjungos **Kriptoturto rinkų reglamentą**, nustatomos procedūros ir kontrolės priemonės, skirtos Klientų Kriptoturto saugiam laikymui ir valdymui. Šios politikos tikslas – sumažinti turto praradimo riziką, užtikrinti tikslų ir išsamų apskaitos tvarkymą bei užtikrinti skaidrumą dėl saugojimo sąlygų ir su tuo susijusių rizikų. Joje taip pat apibrėžiama, kaip Bendrovė saugo Klientų turtą taikydama atskyrimą, prieigos kontrolės priemones ir veiklos tęstinumo planavimą. Politika reguliariai peržiūrima ir atnaujinama, atsižvelgiant į pasikeitusius reglamentavimo reikalavimus, techninę infrastruktūrą ir vidinę praktiką.

Pagrindinės Bendrovės teikiamų saugojimo paslaugų sudedamosios dalys

- **Saugumo priemonės.** Techninės ir procedūrinės kontrolės priemonės, tokios kaip daugiaveiksnis tapatumo nustatymas, raktų šifravimas, prieigos ribojimas ir saugi piniginės architektūra, apsaugo Kliento Kriptoturtą.

- **Naudotojo sąsaja.** Saugus ir patogus Klientų portalas suteikia Klientams galimybę peržiūrėti likučius, inicijuoti lėšų išėmimą ir valdyti prieigą prie sąskaitos su realaus laiko atnaujinimais.

- **Sandorių vykdymas.** Klientų inicijuojami sandoriai yra tikrinami automatinėmis ir rankinėmis priemonėmis, siekiant užtikrinti atitiktį, tikslumą ir saugų pristatymą į blokų grandinę.

- **Atkūrimo paslaugos.** Atkūrimo procesas, apimantis tapatybės patvirtinimą pagal oficialius dokumentus, leidžia Klientams atgauti prieigą prie sąskaitos praradus prisijungimo duomenis.

- **Klientų aptarnavimas.** Pagalba teikiama tiesioginiu pokalbiu darbo valandomis ir el. paštu, o visi užklausimai registruojami Bendrovės Klientų santykių valdymo sistemoje.

- **Be išorinių paslaugų teikėjų.** visos saugojimo ir administravimo funkcijos atliekamos Bendrovės viduje. Jokios trečiosios šalys neturi prieigos prie piniginių ar privačių kriptografinių raktų.

Saugojimo sprendimai

Bendrovė teikia Kriptoturto saugojimo paslaugas kaip integruotą savo veiklos pasiūlymų dalį. Saugojimas yra būtinas kriptovaliutų mokėjimams, konvertavimui iš lėšų į Kriptoturtą ir Kriptoturto išmokėjimams Klientų vardu užtikrinti. Klientų Kriptoturtas laikomas Atskirosiose piniginėse, kurios yra atskirtos nuo Bendrovės turto ir yra visiškai atsekamas Bendrovės techninėse bei apskaitos sistemose.

Naudojamos trijų tipų Atskirosios piniginės:

- Gilios šaltosios piniginės (*angl. Deep Cold Wallets*), kuriose didžioji dalis Kliento Kriptoturto laikoma neprisijungus prie interneto, atskiruose įrenginiuose. Šioms piniginėms reikia 2 iš 3 kelių parašų patvirtinimo ir jos apima saugų fizinį saugojimą ir prieigos protokolus. Raktų medžiaga yra šifruojama, kuriamos jos atsarginės kopijos ir ji pasiekiama tik suderintais kelių įgaliotų darbuotojų veiksmais.

- Šaltosios piniginės (*angl. Cold Wallets*), kurios taip pat laikomos neprisijungus prie interneto ir naudojamos išmokoms Klientams, tokioms kaip lėšų išėmimai ir grąžinimai. Prieiga suteikiama tik įgaliotiems Bendrovės finansų komandos darbuotojams. Sandoriai yra generuojami sistemos ir jiems reikalingi vieno patvirtinimo parašai.

- Karštosios piniginės (*angl. Hot Wallets*), kurios yra prijungtos prie interneto ir naudojamos Klientų įnašams priimti bei didelio dažnio sandoriams vykdyti. Saugumą užtikrina AWS raktų valdymo paslaugos, naudojant prieigos teisių pagal pareigas valdymą, šifravimą ir automatinius įspėjimus.

Visų tipų piniginės yra prižiūrimos taikant griežtas operacines ir kibernetinio saugumo kontrolės priemones, įskaitant kasdienį suderinimą, raktų gyvavimo ciklo procedūras ir nuolatinę stebėseną. Taikomas saugojimo lėšų telkimas, tačiau individualios Kliento teisės realiuoju laiku registruojamos vidinėje apskaitoje. Bendrovės turtas nelaikomas Atskirosiose piniginėse, o Klientų Kriptoturtas niekada nenaudojamas Bendrovės veikloje.

Klientų pozicijų registras

Bendrovė, vadovaudamasi Kriptoturto rinkų reglamentu, tvarko saugų realaus laiko registrą, kuriame fiksuojamas Klientų Kriptoturto laikymas. Kiekvienam Klientui registre skiriama atskira dalis, užtikrinanti, kad nuosavybės teisės būtų aiškiai atskirtos, atsekamos ir prieinamos ataskaitų teikimo bei suderinimo tikslais. Visi sandoriai – įnašai, išėmimai ir vidiniai pervedimai – registruojami pagal Kliento nurodymus ir prieš įvykdymą yra kruopščiai tikrinamas tapatumas, užtikrinama atitiktis ir atliekamos patikros procedūros. Įvykdžius sandorį, jis įrašomas su visa informacija, o Klientui išsiunčiamas patvirtinimas. Klientai gali bet kuriuo metu per Klientų portalą peržiūrėti ataskaitas ir kiekvieną mėnesį gauti Būklės ataskaitą, kurioje nurodomas turimas Kriptoturtas, jo vertė ir likučiai.

Registro techninė architektūra ir duomenų saugojimas

Bendrovės klientų pozicijų registras sukurtas naudojant PostgreSQL duomenų bazę, valdomą per Amazon Web Services (AWS) Relational Database Service (RDS) platformą, užtikrinančią patikimumą, saugumą ir aukštą pasiekiamumą. Sistema apima dvi duomenų bazes: core-ledger, kurioje registruojamos visos finansinės operacijos pagal dvejybinio įrašo principą, ir core-database, kurioje saugoma susijusi informacija apie operacijas ir klientus. Registras veikia tik pridedant įrašus, todėl neleidžiama keisti ar trinti esamų įrašų. Kiekviena operacija pažymima laiko žyma, turi unikalų identifikatorių ir yra registruojama nuosekliai. Duomenų vientisumas užtikrinamas taikant dvejybinę apskaitą, privalomus ryšius tarp lentelių ir unikalius indeksus, kurie neleidžia dubliuoti įrašų. Nuolatinės atsarginės kopijos kuriamos per AWS RDS pagal Bendrovės patvirtintas duomenų atsarginių kopijų kūrimo ir atkūrimo procedūras.

Klientų turto atskyrimas

Bendrovė užtikrina, kad visas Klientų Kriptoturtas būtų laikomas Atskirosiose piniginėse arba apsaugotose sąskaitose, visiškai atskirai nuo Bendrovės nuosavo turto. Šis turtas lieka Kliento nuosavybe ir negali būti naudojamas Bendrovės veiklai, investicijoms ar įsipareigojimams vykdyti. Vidinė apskaita tiksliai fiksuoja kiekvieno Kliento teises, net ir kai turtas yra telkiamas. Prieiga prie Atskirųjų piniginių ar apsaugotų sąskaitų yra griežtai ribojama tik paskirtiems darbuotojams, o visi sandoriai vykdomi laikantis saugumo protokolų, įskaitant daugiaveiksnį tapatumo nustatymą ir šifravimą. Atsitiktinai gavus Kliento turtą į operacinę piniginę, Bendrovė jį perveda į atitinkamą Atskirąją piniginę arba apsaugotą sąskaitą ne vėliau kaip kitą darbo dieną arba priskiria lygiavertį turtą iš nuosavų lėšų. Esant nemokumo situacijai, Kliento turtas yra apsaugotas nuo Bendrovės ieškinių.

Rizikos valdymas

Bendrovė aktyviai identifikuoja, stebi ir mažina su Kriptoturto saugojimu susijusias rizikas. Tai apima neteisėtą prieigą, turto vagystę, techninius gedimus, veiklos klaidas, reguliavimo pažeidimus ir rinkos svyravimus. Kontrolės priemonės apima šifravimą, daugiaveiksnį tapatumo nustatymą, prieigą pagal pareigas, įsibrovimų aptikimą ir reguliarius auditus. Raktų valdymas vykdomas pagal griežtus gyvavimo ciklo protokolus, su saugiu atsarginių kopijų kūrimu ir kelių parašų patvirtinimu. Techninės rizikos yra valdomos taikant stebėsenos priemones, pažeidžiamumo analizę ir išbandytas atkūrimo procedūras. Veiklos atsparumą užtikrina pareigų atskyrimas, darbuotojų mokymai ir incidentų valdymo procedūros. Atitiktis reglamentavimui užtikrinama nuolat stebint teisinę aplinką, atnaujinant politiką ir atliekant audito peržiūras.

Kriptoturtui priskirtų teisių įgyvendinimas

Bendrovė neužtikrina su saugomu Kriptoturtu susijusių teisių įgyvendinimo, tokių kaip balsavimas, įkeitimas, dalyvavimas valdyme ar protokolo atlygių gavimas. Atsiradus atsiskyrimui (*angl. hard fork*), pasiskirstymui (*angl. airdrop*) ar panašiam įvykiui, Klientai neturi teisės į jokią dėl to atsiradusią teisę ar naują turtą, nebent Bendrovė aiškiai nurodo kitaip. Turtas laikomas sutelktose piniginėse, ir joks

individualus paskirstymas ar teisė į naudą, kylančią iš tokių įvykių, nėra suteikiami, išskyrus atvejus, kai Bendrovė savo nuožiūra nusprendžia tokį paskirstymą ar palaikymą užtikrinti.

Prieiga prie saugomo Kriptoturto ir jo grąžinimas

Klientai gali bet kuriuo metu saugiai pasiekti ir atsiimti savo Kriptoturtą per Bendrovės šifruotą Klientų portalą, kuriame taikomas daugiaveiksnis tapatumo nustatymas. Lėšų išėmimo prašymai apdorojami taikant struktūrizuotą ir saugią procedūrą, kuri apima piniginės nuosavybės patvirtinimą, tapatybės nustatymą ir atitikties tikrinimą pagal reglamentavimo reikalavimus. Visa prieigos ir turto grąžinimo veikla yra registruojama, o sąskaitos veiksmai nuolat stebimi siekiant užtikrinti skaidrumą ir sudaryti sąlygas auditui. Jautrioms operacijoms, tokioms kaip sąskaitos saugumo nustatymų keitimas ar naujų lėšų išėmimo adresų pridėjimas, reikalingas papildomas tapatumo patvirtinimas. Praradę prieigos duomenis, Klientai gali inicijuoti saugų atkūrimo procesą, kurio metu patvirtinama tapatybė pateikiant valstybės išduotą asmens tapatybės dokumentą ir patvirtinami sąskaitos duomenys. Tam tikrose situacijose, tokiose kaip nepalaikomas turtas, sąskaitos uždarymas ar priežiūros institucijų nurodymai, Bendrovė gali grąžinti arba likviduoti Kriptoturtą, iš anksto apie tai pranešdama, kai tik įmanoma.

Atsakomybė už Kriptoturto praradimą

Bendrovė atsako už bet kokį Kriptoturto ar prieigos duomenų praradimą, atsiradusį dėl jos aplaidumo, netinkamo elgesio ar sutartų saugumo protokolų nesilaikymo. Atsakomybė yra ribojama prarasto Kriptoturto rinkos verte įvykio metu, nustatyta pagal vidutines kainas pagrindinėse Kriptoturto keitimo platformose. Bendrovė neatsako už nuostolius, atsiradusius dėl Kliento aplaidumo, duomenų vagystės, trečiųjų šalių saugumo pažeidimų, DLT sutrikimų ar *force majeure* aplinkybių. Atsiradus nuostoliui, Bendrovė atliks tyrimą, dokumentuos nustatytas aplinkybes ir informuos nukentėjusius Klientus. Klientai privalo pranešti apie nuostolius per nustatytą laikotarpį. Nustačius Bendrovės atsakomybę, bus išmokėta kompensacija. Bendrovė taip pat laikosi pareigos įgyvendinti veiksmingas saugumo kontrolės priemones, teikti informaciją apie rizikas, užtikrinti darbuotojų mokymus ir tiksliai tvarkyti apskaitą, siekiant užkirsti kelią turto praradimui.