Política de Custódia de Criptoativos

Versão Portuguesa >> Página 3

Crypto-Assets Custody Policy

English Version >> Page 19

Disclaimer:

Em caso de divergência entre as versões, as Partes declaram que prevalece o disposto na versão portuguesa.

In the event of any discrepancy between the versions, the Parties hereby declare that the provisions set forth in the Portuguese version shall prevail

Contents

1. Introdução

A presente política de custódia, administração e segregação de criptoativos e de fundos ("**Política**") foi aprovada pelo Conselho de Administração do Bison Bank, S.A. ("**Bison Bank**" ou "**Banco**") nos termos e para os efeitos dos artigos 70.º, n.º 1, e 75.º, n.º 3 do Regulamento (UE) n.º 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 ("**MiCA**").

2. Enquadramento

Esta Política estabelece as regras e procedimentos internos para assegurar a guarda e o controlo dos criptoativos e dos fundos dos clientes recebidos em custódia pelo Banco, ou dos meios de acesso aos mesmos, bem como os procedimentos de segregação dos criptoativos dos clientes.

Neste sentido, visa-se minimizar o risco de perda dos criptoativos dos clientes, dos direitos associados a esses criptoativos ou dos meios de acesso aos criptoativos devido a situações de fraude, ciber-ameaça ou negligência.

2.1 Âmbito e objetivos

Esta Política estabelece regras e procedimentos internos relativos à prestação pelo Banco aos seus clientes de serviços de custódia e administração de criptoativos em nome de clientes, tal como definidos no MiCA[1], i.e., a conservação ou controlo, em nome de clientes, de criptoativos ou dos meios de acesso a esses criptoativos, quando aplicável sob a forma de chaves criptográficas privadas. A Política estabelece ainda procedimentos relativos à segregação dos fundos de clientes recebidos pelo Banco.

A presente Política é aplicável aos colaboradores e aos membros do Conselho de Administração e do Conselho Fiscal do Banco.

2.2 Definições

Para efeitos da presente Política, são considerados "clientes" todas as pessoas singulares ou coletivas que (i) sejam clientes atuais, (ii) sejam potenciais clientes (i.e., em relação aos quais o Banco procura iniciar uma relação contratual), ou (iii) tenham sido clientes que já terminaram a sua relação contratual com o Banco, mas em relação aos quais esta ainda se mantém vinculada por obrigações pós-contratuais, fiduciárias ou similares.

[1] Artigo 3.º, n.º 1, ponto 17) do MiCA.

3. Documentos referenciados

Este documento é subscrito em simultâneo com as Condições Gerais, e faz parte integrante do acordo celebrado entre o Banco e o Cliente no âmbito da prestação do serviço de custódia e administração de criptoativos, complementando Condições Gerais em tudo o que nelas não se encontre especificamente regulado e disponibilizada em https://www.bisonbank.com.

4. Custódia e administração de criptoativos

a. Contrato com o cliente

Tal como os demais serviços, a prestação de serviços de custódia e administração de criptoativos exige a celebração prévia de um contrato com o cliente que estipule os direitos e obrigações de cada uma das partes, incluindo, pelo menos, os seguintes elementos:

a) A identidade do Banco e do cliente;

b) A natureza dos serviços de criptoativos prestados e uma descrição desses serviços;

c) A presente Política;

d) Os meios de comunicação entre o Banco e o cliente, incluindo o sistema de autenticação do cliente;

e) Uma descrição dos sistemas de segurança utilizados pelo Banco;

f) As comissões, custos e encargos aplicados pelo Banco;

g) A lei aplicável.

Assim, em nenhum caso poderá o Banco prestar serviços de custódia e administração de criptoativos a clientes sem que tenha sido previamente celebrado o respetivo contrato, de acordo com os procedimentos de contratação aplicáveis em cada momento.

A informação pré-contratual a prestar ao cliente pelo Banco deverá alertar para o facto de que os criptoativos não estão abrangidos pelo Sistema de Indemnização aos Investidores nem pelo Fundo de Garantia de Depósitos, pelo que, num cenário de insolvência do Banco, os clientes que sejam tratados como investidores não profissionais não beneficiarão da proteção conferida por aquele sistema ou aquele fundo relativamente aos criptoativos em contas de custódia junto do Banco.

Nos casos em que recorra a outros prestadores de serviços de criptoativos para efetuar a custódia dos criptoativos dos clientes, o Banco deverá informar o cliente desse facto previamente à celebração do contrato, ou se tiver ocorrido apenas após a celebração, assim que ocorra.

b. Registo de criptoativos

O Banco deverá manter um registo das posições abertas em nome de cada cliente correspondentes aos direitos de cada cliente sobre os criptoativos, incluindo o tipo de criptoativo, a quantidade detida e a identificação da carteira correspondente (própria ou de terceiros). Quaisquer movimentos efetuados na sequência de instruções dos clientes deverão ser devidamente inscritos, assim que possível e, no máximo, no prazo de um dia útil, no registo das posições do cliente.

O Banco deverá garantir que qualquer movimento que afete o registo dos criptoativos do cliente é suportado por uma transação devidamente registada no registo de posições do cliente.

c. Prestação de informação durante a prestação do serviço

Sempre que pedido pelos clientes e, pelo menos, trimestralmente, o Banco fornecerá aos mesmos um extrato da conta de custódia que identifique as posições de criptoativos registados em seu nome.

Esse extrato será fornecido em formato eletrónico e identificará (i) os criptoativos do cliente, (ii) o respetivo saldo, (ii) o respetivo valor e (iii) quaisquer transferências de criptoativos efetuadas durante o período em causa.

O pedido de extrato deve ser feito por meio eletrónico, através de uma mensagem segura através da aplicação (*homebanking*) do Banco. Na sequência da receção do pedido, o extrato deverá ser enviado dentro de 10 dias úteis por meio eletrónico, através de uma mensagem segura enviada através da aplicação (*homebanking*) do Banco.

Sempre que uma operação relativa a criptoativos custodiados exija uma resposta por parte do cliente, o Banco presta ao cliente, com a maior brevidade possível e, no máximo, no prazo de 2 dias úteis, as informações de que disponha relativas à mesma.

d. Identificação de criptoativos e de meios de acesso a criptoativos

O Banco adota um sistema de registo e controlo rigorosos para garantir que cada criptoativo custodiado seja corretamente identificado e associado ao cliente respetivo. Os métodos utilizados são:

1) Sistema de registo de ativos: o Banco mantém um sistema de registo interno que identifica detalhadamente os criptoativos de cada cliente (ver acima).
2) Princípio dos 4 olhos e autenticação forte: é assegurada em todos os sistemas de registo e de gestão de carteiras um prática de governação e controlo de qualidade que exige que pelo menos dois indivíduos revejam, aprovem ou autorizem uma decisão, tarefa ou processo, de forma a garantir a responsabilização, reduzir erros e evitar fraudes. Todos os utilizadores são

autenticados por múltiplos fatores para verificar a identidade, normalmente combinando dois ou mais dos seguintes: algo que o utilizador sabe (por exemplo, uma palavra-passe), algo que o utilizador tem (por exemplo, um token de segurança ou um smartphone) e algo que o utilizador é (por exemplo, dados biométricos como uma impressão digital ou reconhecimento facial).

3) **Reconciliações diárias:** processos instituídos para garantir a exatidão e a coerência dos registos financeiros, comparando com os registos em blockchain e documentos comprovativos de contrapartes, para identificar e resolver discrepâncias, caso existam.

Os meios de acesso aos criptoativos, como chaves privadas e informações de autenticação, são tratados com o devido sigilo e segurança, com vista a minimizar o risco de perda dos criptoativos ou dos respetivos meios de acesso. As práticas de custódia desses meios são:

1) **Armazenamento de chaves privadas**: as chaves privadas associadas aos criptoativos dos clientes são geradas e o seu backup armazenado em ambiente seguro, seguindo, e sujeito a, critérios e controlos de segurança frequentes, protegido contra acessos não autorizados, fracionada em diversas partes e com redundância de forma a assegurar a sua restituição a qualquer momento ou eventualidade.
2) **Sistemas de gestão de chaves**: utiliza-se um sistema especializado para gerir infraestrutura de carteiras com tecnologia *Multi-Party Computation* (MPC), a mais avançada tecnologia em termos de segurança para a custódia e gestão das operações diárias. Adicionalmente, é assegurado que outras contrapartes de custódia possuem as devidas certificações exigíveis, nomeadamente ISAE 3000 e ISAE 3402, ou equivalentes.
3) **Princípio dos 4 olhos e autenticação forte**: nos mesmos termos descritos no ponto 2 do parágrafo anterior.

Todas as informações sensíveis, como chaves privadas e credenciais, são protegidas por criptografia, garantindo a confidencialidade e a integridade dos meios de acesso.

e. Exercício de direitos inerentes a criptoativos

Sempre que os criptoativos custodiados atribuam aos seus titulares direitos suscetíveis de ser exercidos, o Banco envidará os seus melhores esforços para facilitar o exercício pelos clientes dos direitos inerentes aos criptoativos.

Para o efeito, assim que tenha conhecimento dos mesmos, o Banco deverá registar de imediato no registo de posições do cliente quaisquer eventos que provavelmente atribuam ou modifiquem direitos dos clientes.

O Banco não está obrigado a manter-se informado sobre quaisquer eventos relacionados com os criptoativos custodiados, cabendo aos clientes monitorizar a existência de eventos que possam criar ou modificar os seus direitos, ou permitir o exercício de direitos.

Os procedimentos a adotar pelo Banco e pelos seus clientes para o exercício de direitos são os seguintes:

1) Notificação de eventos aos clientes: Assim que tenha conhecimento dos mesmos, o Banco deverá informar os clientes sobre quaisquer eventos relevantes que lhes permitam dar instruções ao Banco sobre o exercício de direitos relacionados com os seus criptoativos.
2) Notificação de eventos por parte dos clientes: caso pretendam exercer os direitos inerentes aos seus criptoativos (seja por sua iniciativa ou após uma notificação por parte do Banco), os clientes deverão, sempre que tal seja operacionalmente possível, exercer esses direitos diretamente; caso tal não seja possível, deverão comunicar ao Banco as respetivas instruções de exercício de direitos, de forma completa, precisa e clara, de modo a permitir ao Banco avaliar a natureza e contexto do evento e, em caso de aprovação, desencadear os procedimentos tendentes ao exercício de direitos dos clientes.

No entanto, o contrato entre o Banco e o cliente poderá excluir esse direito. O Banco atuará sempre no melhor interesse dos seus clientes, no entanto, devido à natureza descentralizada das tecnologias de registo distribuído ("DLT"), o Banco poderá não estar imediatamente ciente de *forks*, *airdrops* ou outros eventos que afetem os seus criptoativos. Adicionalmente, o Banco reserva o direito de atrasar ou recusar o suporte para tais eventos se eles representarem riscos de segurança (por exemplo, ciberataques ou *smartcontrats* maliciosos), riscos de PBCFT ou forem incompatíveis com a infraestrutura de carteira ou sistemas técnicos do Banco.

Os clientes reconhecem que as decisões de oferecer suporte a novos *tokens* ou *blockchain* são da exclusiva responsabilidade do Banco, com base em fatores que incluem estabilidade da rede, segurança, liquidez e requisitos de conformidade. Salvo acordo em contrário por escrito, o Banco não será responsável por perdas decorrentes de eventos não suportados, exceto em casos de negligência grave ou conduta dolosa. O Banco comunicará as suas decisões através do site e atualizará o seu registo de posições imediatamente quando novos direitos forem suportados.

A este respeito, quando alterações na DLT impliquem a alteração de alguns dos elementos relativos aos criptoativos do cliente, o Banco, assim que tenha conhecimento dos mesmos, comunica o evento ao cliente para que este tome a sua decisão com o conhecimento necessário, e, na ausência de resposta quanto ao modo de atuar, privilegiará a prática dos atos que, de acordo com critérios de razoabilidade, melhor salvaguardem os criptoativos e a posição do cliente.

Nestes casos, o Banco informa os clientes sobre o evento que vai ocorrer e como o mesmo pode afetar os seus criptoativos, prestando-lhes informações claras e transparentes sobre a atribuição de criptoativos ou a modificação de direitos dele resultantes.

O Banco informa os clientes da forma de exercício dos direitos resultantes desse evento. Todavia, caso os clientes não os exerçam, ou comuniquem ao Banco a decisão de não exercer esses direitos, dentro do prazo previsto para esse evento, o Banco não será responsabilizada pela sua perda, quando esta consequência resulte desse não exercício.

Adicionalmente, o Banco não garante ao cliente que dispõe da capacidade de custódia de criptoativos emergentes do exercício desses direitos (e.g., rede DLT ou criptoativos não suportados, dificuldades de cumprimento dos deveres legais em matéria de registo ou de prevenção de branqueamento de capitais, etc.). Nesses casos, o Banco comunica aos clientes esse facto, informando-os dos procedimentos que podem adotar (e.g., transferência dos criptoativos para um terceiro prestador de serviços de custódia, etc.). Quando o procedimento alternativo escolhido pelo cliente implicar a prestação de serviços de criptoativos pelo Banco, estes estarão sujeitos ao preçário aplicável para cada tipo de serviços em vigor a cada momento.

f. Devolução de criptoativos

O Banco assegura que, caso tal seja expressamente solicitado pelos clientes, os criptoativos dos mesmos, ou os respetivos meios de acesso, lhes são devolvidos com a maior brevidade possível.

O Banco apenas devolve aos clientes criptoativos mediante a transferência para uma *wallet* indicada pelo cliente em causa e que esteja aberta em seu nome junto de um prestador de serviços de criptoativos ou que detenha a sua propriedade (*unhosted wallet*) e faça prova junto do Banco.

Para o efeito, quando o cliente solicite a devolução dos seus criptoativos, o Banco procede, no prazo de um dia útil, à transferência dos mesmos para a *wallet* indicada pelo cliente, após a receção de todas as informações e documentação de suporte necessária solicitada ao cliente no contexto da solicitação em causa.

O Banco está sujeito, em qualquer caso, a cumprir os procedimentos internos previstos na Política de Prevenção de Branqueamento de Capitais e Financiamento de Terrorismo e na Política de Serviços de Transferência que, em situações devidamente justificadas, poderão afetar o prazo indicado.

g. Fontes de risco operacional e de riscos relacionados com tecnologias de informação e comunicação

Existem diversas fontes de riscos operacionais e relacionados com tecnologias da informação e comunicação (TIC) que podem surgir em relação à custódia e administração de criptoativos ou aos meios de acesso aos criptoativos dos clientes. Esses riscos estão relacionados tanto com operações

internas como com ameaças externas, e representam desafios significativos para garantir a segurança e a confiabilidade dos serviços de criptoativos.

O Banco identifica como principais riscos operacionais e de TIC:

1) Ciberataques

O Banco, enquanto prestadora de serviços de criptoativos, pode ser alvo de ataques cibernéticos, como *phishing*, *malware*, *ransomware* ou ataques de negação de serviço distribuído (DDoS), os quais podem comprometer os sistemas e levar à perda de criptoativos ou ao furto de dados sensíveis.

Paralelamente, o acesso não autorizado a dados sensíveis dos clientes (incluindo chaves privadas, senhas ou informações pessoais) pode resultar em perda de confiança e danos financeiros tanto para os clientes quanto para o Banco.

Por forma a mitigar estes riscos, o Banco:

- Implementa sistemas de segurança, como *firewalls* e criptografia avançada.
- Aplica um sistema de autenticação multifator (MFA) para acesso a sistemas sensíveis.
- Treina regularmente os trabalhadores sobre prevenção de *phishing* e boas práticas de segurança.
- Realiza auditorias e testes de segurança para identificar vulnerabilidades.

Os clientes estão também obrigados a guardar adequadamente todas as suas credenciais de acesso, não atuando negligentemente de qualquer forma que possa pôr em causa a segurança da informação.

2) Falhas Tecnológicas e Interrupções

Falhas ou congestionamentos nas infraestruturas subjacentes aos criptoativos, como *software* de *wallets*, *blockchain* ou sistemas de negociação, podem resultar na indisponibilidade temporária ou permanente dos criptoativos dos clientes e em atrasos no processamento de transações.

O *software* utlizado na custódia ou transferência de criptoativos pode conter falhas ou vulnerabilidades que podem ser exploradas por atacantes, levando potencialmente a acessos não autorizados ou perda de criptoativos.

Paralelamente, realidades como *hard forks*, congestionamento da rede ou mudanças nos protocolos de redes *blockchain* específicas podem causar interrupções operacionais.

Por forma a mitigar estes riscos, o Banco:

- Mantem backups redundantes e sistemas de recuperação de desastres para minimizar tempo de inatividade.
- Implementa supervisão contínua de redes e infraestruturas críticas para identificar falhas em tempo real.

- Realiza atualizações de *software* e testes de vulnerabilidade regularmente.
- Define planos de contingência para interrupções causadas por *hard forks* ou congestionamento de *blockchain*.

3) Subcontratação

Falhas ou interrupções na prestação de serviços por prestadores de serviços subcontratados pelo Banco pode levar a interrupções nos serviços prestados pelo Banco ou vulnerabilidades de segurança.

Por forma a mitigar este risco, o Banco:

- Avalia previamente à contratação, e frequentemente ao longo da relação contratual, os prestadores de serviços a quem subcontrate as suas funções, garantindo que cumprem padrões de segurança adequados.
- Celebra contratos robustos com os prestadores de serviços.
- Monitoriza periodicamente a conformidade e o desempenho dos prestadores de serviços.

4) Riscos operacionais

Erros operacionais, tal como a configuração incorreta de sistemas, utilização incorreta de informações sensíveis ou a execução inadequada de transações por parte de colaboradores do Banco, podem resultar na perda de criptoativos.

Por forma a mitigar estes riscos, o Banco:

- Assegura a prestação de formações sobre segurança e melhores práticas operacionais.
- Implementa revisões automatizadas de transações e alertas para reduzir a probabilidade de erros operacionais.

h. Responsabilidade por perda de criptoativos ou meios de acesso aos criptoativos

O Banco não será responsável por perdas de criptoativos ou respetivos meios de acesso resultantes de incidentes que não lhe sejam imputáveis, entendendo-se como tais os eventos que o Banco demonstre terem ocorrido independentemente da prestação do serviço em causa ou das suas operações, e que se situem fora da sua esfera de controlo, nomeadamente problemas inerentes ao funcionamento do registo distribuído que o Banco não controla, incluindo:

- Acesso não autorizado
    - Acesso não autorizado às credenciais de acesso dos clientes à App do Banco, quando esse acesso resulte de facto imputável ao cliente, nomeadamente por negligência do cliente ou incumprimento dos seus deveres de guardar adequadamente as mesmas ou por pôr em causa a segurança da informação.

- Problemas inerentes ao registo distribuído:
    - *Hard forks*, *bugs* ou falhas de segurança inerentes à rede *blockchain* específica utilizada pelos criptoativos custodiados.
    - Congestionamento de rede ou falhas operacionais de *blockchains* que afetam a execução de transações.
    - Mudanças em protocolos ou outras alterações técnicas nas redes *blockchain* que estão fora do controlo do Banco.
- Ataques de terceiros ao Banco ou a qualquer prestador de serviços subcontratado pelo Banco:
    - Ciberataques, incluindo *phishing* ou outros ataques que afetem diretamente o cliente e resultem em perda de criptoativos.
    - Comprometimento de plataformas externas utilizadas pelos clientes para gerir os seus criptoativos.

Qualquer incidente que envolva a perda de criptoativos ou meios de acesso deverá ser imediatamente identificado e relatado ao departamento de *compliance* do Banco. De seguida, uma investigação será conduzida para determinar as causas e avaliar se o incidente é imputável ao Banco.

i. Subcontratação

O Banco apenas poderá recorrer a outros prestadores de serviços de criptoativos que prestem serviços de custódia e administração de criptoativos se esses prestadores de serviços de criptoativos forem autorizados nos termos do artigo 59.º do MiCA.

Atualmente, o Banco recorre ao Sygnum Europe AG (no Liechtenstein) e Circle Internet Financial Europe SAS (em França) .

O Banco implementou um conjunto abrangente de sistemas e controlos para gerir os riscos associados à subcontratação destes serviços.

Previamente à tomada de decisão de subcontratação, o Banco desencadeia um processo de *due diligence*, onde avalia as capacidades do prestador de serviços em causa. Esta metodologia garante que qualquer prestador de serviços a quem seja confiada a responsabilidade de custódia cumpra padrões adequados de integridade operacional e de segurança. O Banco solicita ao prestador de serviços certificações e relatórios periódicos realizados por auditores independentes sobre os controlos de segurança associados ao serviço subcontratado, ex: ISAE3000, ISAE3402, SOC1 e SOC2.

Encontram-se ainda implementados mecanismos internos de monitorização que permitem a avaliação contínua dos contratos de prestação de serviços, neles se incluindo avaliações de risco

regulares, que analisam os riscos operacionais, legais e financeiros associados à subcontratação. O Banco tem ainda implementados planos de contingência e estratégias de saída no caso de um prestador de serviços deixar de reunir as condições necessárias à prestação do respetivo serviço.

Sempre que o Banco subcontrate junto de terceiros prestadores de serviços o exercício de funções que envolvam ou relativas aos serviços de custódia e administração de criptoativos, deverá ainda cumprir com o disposto na Política de Subcontratação.

No âmbito da custódia e administração de criptoativos, o Bison Bank mantém integralmente a responsabilidade fiduciária e regulatória perante os clientes e as autoridades competentes, bem como a relação com os clientes e o controlo dos riscos associados. O Banco é responsável pela definição e aplicação das políticas de custódia, pela gestão de risco, pela supervisão das atividades delegadas, pela segregação contabilística dos ativos, bem como pela realização das reconciliações globais e do reporting operacional e regulatório aplicável.

A Sygnum Europe AG e a Circle Internet Financial Europe SAS executam exclusivamente funções técnicas e operacionais claramente delimitadas, atuando sempre sob instrução do Banco, sem qualquer poder de decisão comercial ou de gestão de risco. As funções delegadas incluem, nomeadamente, a guarda técnica de criptoativos, a execução técnica de transferências no âmbito dos respetivos serviços e a manutenção da segregação técnica dos ativos. As referidas entidades não assumem responsabilidades fiduciárias nem regulatórias perante os clientes, permanecendo tais responsabilidades exclusivamente na esfera do Bison Bank.

No âmbito da prestação de serviços de custódia e administração de criptoativos, a Sygnum Europe AG e a Circle Internet Financial Europe SAS não recorrem a quaisquer subdelegados para a execução das funções técnicas e operacionais que lhes são delegadas pelo Bison Bank, não existindo qualquer subdelegação adicional. O Banco assegura o controlo de risco através de relatórios de garantia independentes (assurance reports), designadamente relatórios ISAE 3402 ou SOC 2, que permitem avaliar a adequação e a eficácia dos controlos técnicos e operacionais implementados pelos prestadores delegados.

Conflitos de interesses decorrentes da subcontratação a terceiros para prestação de serviços de custódia e administração de criptoativos:

O recurso aos prestadores **Sygnum Europe AG** e **Circle Internet Financial Europe SAS** para a execução de funções de custódia e administração de criptoativos pode originar potenciais conflitos de interesse, designadamente:

a) **Assimetria de Informação**

Os prestadores podem deter mais informação técnica, operacional e de risco do que o Banco, criando:

- dificuldade de supervisão plena e independente por parte do Banco;
- dependência excessiva de informação fornecida pelo prestador;
- limitações na capacidade de avaliar incidentes de segurança ou falhas operacionais.

Medidas de mitigação

- Due diligence reforçada prévia à contratação e periódica (certificações ISAE 3000, ISAE 3402, SOC 1, SOC 2).
- Reuniões técnicas recorrentes entre equipas do Banco e dos prestadores.
- Obrigações contratuais de transparência e disponibilização de evidências operacionais.

b) Conflitos de Prioridade e Alocação de Recursos

Sygnum e Circle prestam serviços a múltiplas instituições financeiras, podendo:

- prioritizar outros clientes ou atividades mais lucrativas;
- afetar os tempos de resposta ou qualidade do serviço prestado ao Banco.

Medidas de mitigação

- Mecanismos de escalamento para incidentes críticos.
- Monitorização contínua do desempenho e registo de incidentes.

c) Dependência Operacional e Risco de Concentração

Delegar custódia a terceiros aumenta a dependência operacional, incluindo:

- risco de interrupção ou falhas nos sistemas do prestador;
- dificuldade de substituir rapidamente o prestador em caso de falha grave.

Medidas de mitigação

- Definição de planos de continuidade de negócio e planos de saída (exit plans).
- Acompanhamento periódico dos riscos de concentração.
- Verificação de que os prestadores cumprem requisitos MiCA (art. 59.º).

d) Divergências nos Padrões de Segurança

O nível de segurança exigido pelo Banco pode não coincidir com os controlos internos dos prestadores, nomeadamente:

- gestão de chaves criptográficas;
- segregação de carteiras;

Medidas de mitigação

- Obrigações contratuais de cumprimento de requisitos mínimos de segurança.
- Auditorias independentes exigidas ao prestador (ISAE 3000, ISAE 3402, SOC 1, SOC 2)

A delegação de funções de custódia à Sygnum Europe AG e à Circle Internet Financial Europe SAS implica riscos e potenciais conflitos de interesses que o Bison Bank identifica, monitoriza e mitiga através de controlos contratuais, operacionais, de governance e tecnológicos alinhados com o Regulamento (UE) 2023/1114 (MiCA) e com as orientações da ESMA sobre conflitos de interesse para CASPs. Adicionalmente, e com vista a mitigar estas e outras situações, o Banco dispõe de procedimentos específicos e adequados para identificar, prevenir, gerir e divulgar quaisquer conflitos de interesses, reais ou potenciais, nos termos descritos na Política de Prevenção e Gestão de Conflitos de Interesses em vigor no Banco.

j. Serviços de *staking*

O *staking* é o processo de imobilização de criptoativos para apoiar as operações de mecanismos de consenso de *blockchain* baseadas em *proof-of-stake* e mecanismos semelhantes, em troca da concessão de privilégios de validação que podem gerar recompensas de bloco[2].

O Banco presta aos seus clientes serviços de *staking* (também conhecidos como *staking-as-a-service*), mediante remuneração, ao abrigo dos quais se compromete a fazer o *staking* dos criptoativos dos clientes em seu nome. O Banco receberá, em nome do cliente, o rendimento ou obterá os privilégios de validação que lhe permitem ganhar recompensas de bloco.

Esse rendimento ou essas recompensas de bloco são distribuídas ao cliente, podendo o Banco reter, como remuneração pelo serviço prestado (incluindo, sem limitar, pela prestação de serviços como a realização do *staking* dos criptoativos em nome do cliente, exercer as obrigações de validação, reclamar as recompensas de bloco, etc.), os montantes previamente acordados, conforme estipulado no contrato.

[2] De acordo com a ESMA, em resposta ao Q&A n.º_2067.

Na prestação de serviços de *staking*, os criptoativos, ou as chaves privadas de acesso aos mesmos, são mantidos em custódia pelo Banco. Assim, a prestação de serviços de *staking* é acessória aos serviços de custódia prestados pelo Banco aos clientes. Portanto, ao oferecer e prestar os serviços de *staking*, o Banco cumpre sempre os requisitos estabelecidos no MiCA e na presente Política relativamente à custódia e administração de criptoativos em nome dos clientes.

Em particular, quando os serviços de *staking* são prestados em combinação com a prestação de serviços de custódia, o Banco assegura que os criptoativos mantidos em nome dos clientes possam ser devolvidos, e que o Banco permanece responsável perante os seus clientes por qualquer perda de criptoativos que lhe seja imputável.

Quando os serviços de *staking* são prestados em combinação com quaisquer outros serviços de criptoativos para os quais o Banco esteja autorizada, o Banco deve obter o consentimento explícito dos clientes para fazer o *staking* dos seus criptoativos, uma vez que isso pode ter um impacto na capacidade dos clientes de aceder a esses ativos.

k. Valorização de criptoativos

A valorização rigorosa dos criptoativos é fundamental para assegurar a correta aferição do valor global do portfolio dos clientes, das comissões de custódia a aplicar e de outros encargos associados, garantindo transparência, equidade e alinhamento com as práticas do banco. O método de valorização adotado para os criptoativos sob custódia é realizado de forma idêntica aos ativos tradicionais financeiros no banco. Baseia-se nas valorizações obtidas da Bloomberg que fornece por meio do seu preço genérico proprietário Bloomberg Generic Price (BGN), um composto calculado a partir de cotações obtidas de um conjunto cuidadosamente selecionado de plataformas de negociação de criptoativos que atendem a rigorosos padrões institucionais.

l. Sistemas de segurança aplicáveis ao serviço de custódia

No âmbito da prestação do serviço de custódia e administração de criptoativos, o Banco adota sistemas, procedimentos e mecanismos de segurança adequados à proteção dos criptoativos dos clientes e dos respetivos meios de acesso, cuja concretização operacional se encontra detalhada nos pontos 3 d), 3g) e 4 b) ii) da presente Política.

5. Segregação de criptoativos

a. Segregação de fundos

Enquanto instituição de crédito autorizada e registada junto do Banco de Portugal, o Banco recebe fundos (notas, moedas, moeda fiduciária escritural) dos respetivos clientes. Nestes termos, o Banco cumpre todos os procedimentos relativos à sua atividade de instituição de crédito, nomeadamente no que diz respeito a serviços de pagamento, contas de depósito à ordem e numerário.

Uma vez que o Bison Bank é uma instituição de crédito, está sujeito a requisitos prudenciais, incluindo os estabelecidos no Regime Geral das Instituições de Crédito e Sociedades Financeiras ("**RGICSF**") - que transpõe, entre outras, a Diretiva 2013/36/UE ("**CRD IV**") e a Diretiva 2014/59/UE ("**BRRD**") - o Regulamento (UE) 575/2013 ("**CRR**") e o Regulamento Delegado (UE) 2015/61 da Comissão, incluindo aqueles relativos à gestão de liquidez, alavancagem e risco de ativos, que visam assegurar a solidez da instituição e, consequentemente, a proteção dos seus credores, incluindo depositantes.

As regras prudenciais emergentes do RGICSF, da CRD IV, da BRRD, do CRR e demais regulamentos delegados determinam, entre outros aspetos, que as instituições de crédito implementem medidas que assegurem a manutenção de fundos próprios mínimos, restrições de alavancagem e liquidez suficiente para garantir uma situação financeira robusta e prudente. Assim, o Bison Bank está obrigado a manter caixa ou ativos líquidos de elevada qualidade em quantidades suficientes para cobrir os créditos dos seus clientes.

Desta forma, os clientes estarão salvaguardados porque o Bison Bank manterá em permanência rácios que cobrem todas as suas responsabilidades, entre as quais os direitos de crédito sobre os fundos depositados pelos clientes junto do Banco.

b. Segregação de criptoativos

i. Princípios gerais

Como qualquer ativo que o Banco recebe em custódia dos seus clientes (incluindo instrumentos financeiros, no âmbito da sua atividade de intermediário financeiro), o Banco segrega os criptoativos dos seus clientes dos seus próprios ativos, assegurando que os meios de acesso aos criptoativos dos seus clientes são claramente identificados como tal. Para o efeito, o Banco segrega tanto os criptoativos detidos, como os respetivos meios de acesso, através da sua custódia em contas globais ("contas jumbo") com o registo informático da titularidade pelo cliente a que respeita.

O Banco dispõe de um registo de posições dos criptoativos dos clientes, sendo que os criptoativos pertencem aos clientes e não integram o património e o balanço do Banco, pelo que, num cenário de insolvência do Banco, os direitos aos criptoativos dos clientes devem ser salvaguardados, não integrando a massa insolvente do Banco.

O Banco está expressamente proibido de realizar qualquer tipo de operações por conta própria com criptoativos dos seus clientes.

A segregação visa principalmente tutelar a segurança dos clientes, por forma a que num eventual caso de, e.g., execução ao Banco ou insolvência do Banco, os criptoativos dos clientes estejam salvaguardados e fora do alcance dos credores do Banco no âmbito dos ativos a penhorar ou ser apreendidos para a massa insolvente. Por este motivo, os criptoativos detidos em custódia são juridicamente segregados do património do Banco, no interesse dos clientes, não podendo eventuais

credores do Banco satisfazer-se de quaisquer dívidas desta através dos criptoativos de clientes custodiados no Banco.

ii. *Wallets*

Os criptoativos detidos em nome dos clientes não são utilizados, em caso algum, pelo Banco por conta própria. O Banco assegura nos seus processos internos regulares e de auditoria que todos os fundos são detidos em rácio 1:1 por verificação regular de provas de fundos nas diversas carteiras sob a sua gestão.

No que respeita aos criptoativos dos clientes, o Banco assegura que, nos casos em que os mesmos sejam detidos cumulativamente em contas globais ("contas jumbo"), através dos seus registos informáticos consegue identificar e reproduzir os criptoativos pertencentes a cada cliente. Para o efeito, o Banco implementou um sistema de gestão de títulos no seu sistema core que permite identificar qual o montante de ativos pertencente a cada cliente e sua localização.

iii. Sistema de aprovação de chaves e de salvaguarda de chaves criptográficas

A segurança das chaves criptográficas é um elemento essencial que levou o Banco a estabelecer um sistema abrangente para a aprovação e salvaguarda de chaves criptográficas, com um foco específico em tecnologia MPC, com o objetivo de garantir um elevado nível de segurança e integridade operacional.

No que respeita à aprovação de transações criptográficas são asseguradas diversas políticas de transação por ativo, montante e tipologia, requerendo sempre uma aprovação de pelo menos dois responsáveis das operações.

No que respeita à salvaguarda de chaves criptográficas, estas são fragmentadas e mantidas em dispositivos encriptados, não conectáveis à internet e armazenadas em diferentes locais geográficos, de modo a evitar a perda completa em caso de violação de segurança.

6. Aprovação e disponibilização aos clientes

A presente Política foi aprovada pelo Conselho de Administração em 29 de Junho de 2026 com efeitos imediatos a partir da sua publicação.

Deve ser disponibilizado aos clientes, a pedido destes, um resumo da política de custódia em formato eletrónico.

Contents

1. Introduction

This policy on the custody, management and segregation of crypto-assets and funds ("Policy") has been approved by the Board of Directors of Bison Bank, S.A. (**"Bison** Bank" or **"the Bank"**) in accordance with and for the purposes of Articles 70(1) and 75(3) of Regulation (EU) No 2023/1114 of the European Parliament and of the Council of 31 May 2023 ("MiCA").

2. Scope

This Policy sets out the internal rules and procedures to ensure the safekeeping and control of clients' crypto-assets and funds held in custody by the Bank, or the means of access to them, as well as the procedures for the segregation of clients' crypto-assets.

To this end, the aim is to minimise the risk of loss of clients' crypto-assets, the rights associated with those crypto-assets, or the means of access to the crypto-assets due to fraud, cyber threats or negligence.

2.3 Scope and objectives

This Policy sets out internal rules and procedures relating to the Bank's provision of crypto-asset custody and management services to its clients on their behalf, as defined in MiCA[3] , i.e. the holding or control, on behalf of clients, of crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys. The Policy also sets out procedures relating to the segregation of client funds received by the Bank.

This Policy applies to the Bank's employees and to the members of its Board of Directors and Audit Committee.

2.4 Definitions

For the purposes of this Policy, 'clients' are defined as any natural or legal persons who (i) are current clients, (ii) are potential clients (i.e. in respect of whom the Bank seeks to enter into a contractual relationship), or (iii) have been clients who have already terminated their contractual relationship with the Bank, but in respect of whom the Bank remains bound by post-contractual, fiduciary or similar obligations.

3. Documents referred to

[3] Article 3(1)(17) of MiCA.

This document is entered into simultaneously with the General Terms and Conditions, and forms an integral part of the agreement concluded between the Bank and the Client in relation to the provision of the crypto-asset custody and management service, supplementing the General Terms and Conditions in all matters not specifically regulated therein and available at https://www.bisonbank.com.

4. Custody and management of crypto-assets

a. Agreement with the client

As with other services, the provision of crypto-asset custody and management services requires the prior conclusion of a contract with the customer setting out the rights and obligations of each party, including, at a minimum, the following elements:

h) The identity of the Bank and the client;

i) The nature of the crypto-asset services provided and a description of those services;

j) This Policy;

k) The means of communication between the Bank and the client, including the client authentication system;

l) A description of the security systems used by the Bank;

m) The fees, costs and charges applied by the Bank;

n) The applicable law.

Accordingly, under no circumstances may the Bank provide crypto-asset custody and management services to customers without first having entered into the relevant contract, in accordance with the contracting procedures applicable at any given time.

The pre-contractual information to be provided to the client by the Bank must draw attention to the fact that crypto-assets are not covered by the Investor Compensation Scheme or the Deposit Guarantee Fund; consequently, in the event of the Bank's insolvency, clients treated as retail investors will not benefit from the protection afforded by that scheme or that fund in respect of crypto-assets held in custody accounts with the Bank.

Where the Bank uses other crypto-asset service providers to hold clients' crypto-assets in custody, it must inform the client of this fact prior to the conclusion of the contract, or, if this has only occurred after the contract has been concluded, as soon as it does so.

b. Record-keeping for crypto-assets

The Bank must maintain a register of open positions in each client's name corresponding to each client's rights over the crypto-assets, including the type of crypto-asset, the quantity held and the identification of the corresponding wallet (whether the Bank's own or that of a third party). Any transactions carried out following clients' instructions must be duly recorded, as soon as possible and, at the latest, within one working day, in the client's position register.

The Bank must ensure that any transaction affecting the record of a client's crypto-assets is supported by a transaction duly recorded in the client's position register.

c. Provision of information whilst the service is being provided

Whenever requested by clients, and at least quarterly, the Bank shall provide them with a custody account statement identifying the crypto-asset positions held in their name.

This statement will be provided in electronic format and will identify (i) the customer's crypto-assets, (ii) the respective balance, (iii) the respective value and (iv) any transfers of crypto-assets made during the period in question.

The request for a statement must be made electronically, via a secure message sent through the Bank's *online* banking application. Upon receipt of the request, the statement must be sent within 10 working days electronically, via a secure message sent through the Bank's *online banking* application.

Whenever a transaction relating to custodied crypto-assets requires a response from the customer, the Bank shall provide the customer, as soon as possible and within a maximum of 2 working days, with the information it holds in relation to that transaction.

d. Identification of crypto-assets and means of accessing crypto-assets

The Bank employs a rigorous record-keeping and control system to ensure that each custodied crypto-asset is correctly identified and linked to the relevant customer. The methods used are:

4) Asset registration system: the Bank maintains an internal registration system that identifies each customer's crypto-assets in detail (see above).
5) Four-eyes principle and strong authentication: a governance and quality control practice is ensured across all record-keeping and portfolio management systems, requiring at least two individuals to review, approve or authorise a decision, task or process, in order to ensure accountability, reduce errors and prevent fraud. All users are authenticated using multi-factor authentication to verify their identity, typically combining two or more of the following: something the user knows (e.g. a password), something the user has (e.g. a security token or

a smartphone) and something the user is (e.g. biometric data such as a fingerprint or facial recognition).

6) **Daily reconciliations:** processes put in place to ensure the accuracy and consistency of financial records by comparing them with blockchain records and supporting documents from counterparties, in order to identify and resolve any discrepancies.

Means of access to crypto-assets, such as private keys and authentication details, are treated with due confidentiality and security, with a view to minimising the risk of loss of the crypto-assets or the respective means of access. The custody practices for these means are:

4) **Storage of private keys**: the private keys associated with clients' crypto-assets are generated and their backups stored in a secure environment, in accordance with, and subject to, frequent security criteria and controls, protected against unauthorised access, split into several parts and with redundancy to ensure their recovery at any time or in any eventuality.

5) **Key management systems**: a specialised system is used to manage the wallet infrastructure using *Multi-Party Computation* (MPC) technology, the most advanced security technology for custody and the management of day-to-day operations. In addition, it is ensured that other custody counterparties hold the necessary certifications, namely ISAE 3000 and ISAE 3402, or equivalent.

6) **Four-eyes principle and strong authentication**: as described in point 2 of the previous paragraph.

All sensitive information, such as private keys and credentials, is protected by encryption, ensuring the confidentiality and integrity of access methods.

e. Exercise of rights attached to crypto-assets

Wherever the crypto-assets held in custody confer on their holders rights that may be exercised, the Bank shall use its best endeavours to facilitate the exercise by clients of the rights inherent in the crypto-assets.

To this end, as soon as it becomes aware of such events, the Bank must immediately record in the client's position register any events that are likely to confer or modify clients' rights.

The Bank is under no obligation to keep itself informed of any events relating to the custodied crypto-assets; it is the responsibility of clients to monitor the occurrence of events that may create or modify their rights, or enable the exercise of rights.

The procedures to be followed by the Bank and its clients for the exercise of rights are as follows:

3) Notification of events to clients: As soon as it becomes aware of them, the Bank must inform clients of any relevant events that enable them to give instructions to the Bank regarding the exercise of rights relating to their crypto-assets.

4) Notification of events by clients: should clients wish to exercise the rights attached to their crypto-assets (whether on their own initiative or following notification by the Bank), they must, wherever operationally possible, exercise those rights directly; if this is not possible, they must provide the Bank with their instructions for exercising those rights in a complete, precise and clear manner, so as to enable the Bank to assess the nature and context of the event and, if approved, to initiate the procedures necessary for the exercise of the clients' rights.

However, the contract between the Bank and the customer may exclude this right. The Bank will always act in the best interests of its customers; however, due to the decentralised nature of distributed ledger technologies ('DLT'), the Bank may not be immediately aware of *forks*, *airdrops* or other events affecting its crypto-assets. Furthermore, the Bank reserves the right to delay or refuse support for such events if they pose security risks (for example, cyber-attacks or malicious *smart contracts*), PBCFT risks, or are incompatible with the Bank's wallet infrastructure or technical systems.

Customers acknowledge that decisions to support new *tokens* or *blockchains* are the sole responsibility of the Bank, based on factors including network stability, security, liquidity and compliance requirements. Unless otherwise agreed in writing, the Bank shall not be liable for losses arising from unsupported events, except in cases of gross negligence or wilful misconduct. The Bank will communicate its decisions via its website and update its position register immediately when new rights are supported.

In this regard, where changes to the DLT result in alterations to certain elements relating to the client's crypto-assets, the Bank, as soon as it becomes aware of such changes, shall notify the client of the event so that the client may make an informed decision, and, in the absence of a response regarding how to proceed, the Bank will prioritise taking the actions which, in accordance with reasonable criteria, best safeguard the client's crypto-assets and position.

In such cases, the Bank informs clients of the event that is about to occur and how it may affect their crypto-assets, providing them with clear and transparent information regarding the allocation of crypto-assets or any resulting changes to their rights.

The Bank informs clients of the procedure for exercising the rights arising from such an event. However, should clients fail to exercise these rights, or notify the Bank of their decision not to exercise them, within the timeframe specified for that event, the Bank shall not be held liable for any loss incurred where such a consequence results from this failure to exercise the rights.

Furthermore, the Bank does not guarantee to the customer that it has the capacity to hold in custody any crypto-assets arising from the exercise of these rights (e.g. DLT networks or unsupported crypto-assets, difficulties in complying with legal obligations regarding registration or the prevention of money laundering, etc.). In such cases, the Bank shall notify customers of this fact, informing them of the procedures they may adopt (e.g., transferring the crypto-assets to a third-party custody service provider, etc.). Where the alternative procedure chosen by the customer involves the Bank providing crypto-asset services, these shall be subject to the price list applicable to each type of service in force at any given time.

f. Return of crypto-assets

The Bank ensures that, should customers expressly request it, their crypto-assets, or the means of access thereto, are returned to them as soon as possible.

The Bank will only return crypto-assets to customers by transferring them to a *wallet* specified by the customer in question, which is held in their name with a crypto-asset service provider or which is owned by the customer (*unhosted wallet*), and for which the customer provides proof to the Bank.

To this end, when a customer requests the return of their crypto-assets, the Bank shall, within one working day, transfer them to the *wallet* specified by the customer, following receipt of all the necessary information and supporting documentation requested from the customer in connection with the request in question.

The Bank is, in any event, required to comply with the internal procedures set out in the Anti-Money Laundering and Counter-Terrorist Financing Policy and the Funds Transfer Services Policy, which, in duly justified circumstances, may affect the timeframe indicated.

g. Sources of operational risk and risks related to information and communication technologies

There are various sources of operational risks and risks related to information and communication technologies (ICT) that may arise in connection with the custody and administration of crypto-assets or the means of accessing clients' crypto-assets. These risks relate to both internal operations and external threats, and pose significant challenges to ensuring the security and reliability of crypto-asset services.

The Bank identifies the following as the main operational and ICT risks:

5) Cyberattacks

As a provider of crypto-asset services, the Bank may be the target of cyberattacks, such as *phishing*, *malware*, *ransomware* or distributed denial-of-service (DDoS) attacks, which may compromise systems and lead to the loss of crypto-assets or the theft of sensitive data.

At the same time, unauthorised access to sensitive customer data (including private keys, passwords or personal information) may result in a loss of trust and financial damage to both customers and the Bank.

In order to mitigate these risks, the Bank:

- Implements security systems, such as *firewalls* and advanced encryption.
- Applies a multi-factor authentication (MFA) system for access to sensitive systems.
- Regularly trains staff on *phishing* prevention and good security practices.
- Carries out security audits and tests to identify vulnerabilities.

Customers are also required to store all their access credentials securely and must not act negligently in any way that could compromise information security.

6) Technical Failures and Disruptions

Failures or congestion in the infrastructure underpinning crypto-assets, such as *wallet software*, *blockchain* or trading systems, may result in the temporary or permanent unavailability of clients' crypto-assets and delays in the processing of transactions.

The *software* used for the custody or transfer of crypto-assets may contain faults or vulnerabilities that could be exploited by attackers, potentially leading to unauthorised access or the loss of crypto-assets.

At the same time, factors such as *hard forks*, network congestion or changes to the protocols of specific *blockchain* networks may cause operational disruptions.

In order to mitigate these risks, the Bank:

- Maintains redundant backups and disaster recovery systems to minimise downtime.
- Implements continuous monitoring of critical networks and infrastructure to identify faults in real time.
- Carries out regular *software* updates and vulnerability tests.
- Establishes contingency plans for disruptions caused by *hard forks* or *blockchain* congestion.

7) Outsourcing

Failures or disruptions in the provision of services by service providers subcontracted by the Bank may lead to disruptions in the services provided by the Bank or security vulnerabilities.

To mitigate this risk, the Bank:

- Assesses, prior to engagement and frequently throughout the contractual relationship, the service providers to whom it outsources its functions, ensuring that they meet appropriate security standards.
- Enters into robust contracts with service providers.
- Periodically monitors the compliance and performance of service providers.

8) Operational risks

Operational errors, such as incorrect system configuration, misuse of sensitive information or the improper execution of transactions by the Bank's staff, may result in the loss of crypto-assets.

To mitigate these risks, the Bank:

- Ensures that training on security and best operational practices is provided.
- Implements automated transaction reviews and alerts to reduce the likelihood of operational errors.

h. Liability for loss of crypto-assets or means of access to crypto-assets

The Bank shall not be liable for any loss of crypto-assets or the means of access thereto resulting from incidents for which it is not responsible, such incidents being understood to mean events which the Bank demonstrates have occurred independently of the provision of the service in question or its operations, and which lie outside its sphere of control, namely problems inherent in the functioning of the distributed ledger which the Bank does not control, including:

- Unauthorised access
    - Unauthorised access to customers' login credentials for the Bank's App, where such access is in fact attributable to the customer, in particular due to the customer's negligence or failure to fulfil their duty to safeguard them properly, or by compromising information security.
- Issues inherent to the distributed ledger:
    - *Hard forks*, *bugs* or security flaws inherent to the specific *blockchain* network used by the custodial crypto-assets.
    - Network congestion or operational failures of *blockchains* that affect the execution of transactions.
    - Changes to protocols or other technical alterations to *blockchain* networks that are beyond the Bank's control.
- Attacks by third parties on the Bank or any service provider subcontracted by the Bank:

- Cyberattacks, including *phishing* or other attacks that directly affect the customer and result in the loss of crypto-assets.
- Compromise of external platforms used by customers to manage their crypto-assets.

Any incident involving the loss of crypto-assets or means of access must be immediately identified and reported to the Bank's *compliance* department. An investigation will then be conducted to determine the causes and assess whether the incident is attributable to the Bank.

i. Outsourcing

The Bank may only engage other crypto-asset service providers that offer crypto-asset custody and administration services if such crypto-asset service providers are authorised under Article 59 of MiCA.

Currently, the Bank uses Sygnum Europe AG (in Liechtenstein) and Circle Internet Financial Europe SAS (in France).

The Bank has implemented a comprehensive set of systems and controls to manage the risks associated with the outsourcing of these services.

Prior to deciding to outsource, the Bank initiates a *due diligence* process to assess the capabilities of the service provider in question. This methodology ensures that any service provider entrusted with custodial responsibility meets appropriate standards of operational integrity and security. The Bank requires the service provider to submit certifications and periodic reports prepared by independent auditors on the security controls associated with the outsourced service, e.g. ISAE 3000, ISAE 3402, SOC 1 and SOC 2.

Internal monitoring mechanisms are also in place to enable the ongoing assessment of service agreements, including regular risk assessments that analyse the operational, legal and financial risks associated with outsourcing. The Bank has also implemented contingency plans and exit strategies in the event that a service provider ceases to meet the necessary conditions for the provision of the relevant service.

Whenever the Bank subcontracts to third-party service providers the performance of functions involving or relating to the custody and administration of crypto-assets, it must also comply with the provisions of the Subcontracting Policy.

In the context of the custody and administration of crypto-assets, Bison Bank retains full fiduciary and regulatory responsibility towards clients and the competent authorities, as well as the client relationship and the management of associated risks. The Bank is responsible for defining and implementing custody policies, for risk management, for supervising delegated activities, for the accounting segregation of assets, as well as for carrying out overall reconciliations and the applicable operational and regulatory reporting.

Sygnum Europe AG and Circle Internet Financial Europe SAS perform exclusively clearly defined technical and operational functions, acting at all times on the Bank's instructions, without any commercial or risk management decision-making powers. The delegated functions include, in particular, the technical safekeeping of crypto-assets, the technical execution of transfers within the scope of the respective services, and the maintenance of the technical segregation of assets. These entities do not assume any fiduciary or regulatory responsibilities towards clients; such responsibilities remain exclusively with Bison Bank.

In the provision of crypto-asset custody and administration services, Sygnum Europe AG and Circle Internet Financial Europe SAS do not use any sub-delegates to carry out the technical and operational functions delegated to them by Bison Bank; there is no further sub-delegation. The Bank ensures risk control through independent assurance reports, namely ISAE 3402 or SOC 2 reports, which enable the adequacy and effectiveness of the technical and operational controls implemented by the delegated service providers to be assessed.

Conflicts of interest arising from the outsourcing of crypto-asset custody and administration services to third parties:

The use of service providers **Sygnum Europe AG** and **Circle Internet Financial Europe SAS** to carry out crypto-asset custody and administration functions may give rise to potential conflicts of interest, namely:

e) Information asymmetry

The service providers may hold more technical, operational and risk-related information than the Bank, creating:

- difficulty for the Bank to exercise full and independent supervision;
- excessive reliance on information provided by the service provider;
- limitations on the ability to assess security incidents or operational failures.

Mitigation measures

- Enhanced due diligence prior to engagement and on a regular basis (**ISAE 3000**, **ISAE 3402**, **SOC 1** and **SOC 2** certifications).

- Regular technical meetings between the Bank's teams and those of the service providers.
- Contractual obligations regarding transparency and the provision of operational evidence.

f) Conflicts of Priority and Resource Allocation

Sygnum and Circle provide services to multiple financial institutions and may:

- prioritise other clients or more profitable activities;
- affect response times or the quality of the service provided to the Bank.

Mitigation measures

- Escalation procedures for critical incidents.
- Continuous performance monitoring and incident logging.

g) Operational Dependency and Concentration Risk

Delegating custody to third parties increases operational dependency, including:

- the risk of disruption or failure in the provider's systems;
- difficulty in quickly replacing the provider in the event of a serious failure.

Mitigation measures

- Establishment of business continuity plans and exit plans.
- Regular monitoring of concentration risks.
- Verification that service providers comply with MiCA requirements (Article 59).

h) Discrepancies in Security Standards

The level of security required by the Bank may not align with service providers' internal controls, in particular:

- cryptographic key management;
- portfolio segregation;

Mitigation measures

- Contractual obligations to comply with minimum security requirements.
- Independent audits required of the service provider (ISAE 3000, ISAE 3402, SOC 1, SOC 2)

The delegation of custody functions to Sygnum Europe AG and Circle Internet Financial Europe SAS entails risks and potential conflicts of interest which Bison Bank identifies, monitors and mitigates through contractual, operational, governance and technological controls aligned with Regulation (EU) 2023/1114 (MiCA) and with ESMA's guidelines on conflicts of interest for CASPs. Furthermore, with a view to mitigating these and other situations, the Bank has specific and appropriate procedures in place to identify, prevent, manage and disclose any actual or potential conflicts of interest, in accordance with the terms set out in the Bank's current Policy on the Prevention and Management of Conflicts of Interest.

j. *Staking* services

Staking is the process of locking up crypto-assets to support the operations of *blockchain* consensus mechanisms based on *proof-of-stake* and similar mechanisms, in exchange for the granting of validation privileges that may generate block rewards[4] .

The Bank provides its clients with *staking* services (also known as *staking-as-a-service*), in return for a fee, under which it undertakes to *stake* clients' crypto-assets on their behalf. The Bank will receive, on behalf of the client, the yield or obtain the validation privileges that enable it to earn block rewards.

This income or these block rewards are distributed to the customer, and the Bank may retain, as remuneration for the service provided (including, but not limited to, the provision of services such as *staking* the crypto-assets on the customer's behalf, performing validation obligations, claiming block rewards, etc.), the amounts previously agreed, as stipulated in the contract.

When providing *staking* services, the crypto-assets, or the private keys granting access to them, are held in custody by the Bank. Thus, the provision of *staking* services is ancillary to the custody services provided by the Bank to clients. Consequently, when offering and providing *staking* services, the Bank always complies with the requirements set out in MiCA and in this Policy regarding the custody and administration of crypto-assets on behalf of clients.

In particular, where *staking* services are provided in conjunction with custody services, the Bank ensures that the crypto-assets held on behalf of clients can be returned, and that the Bank remains liable to its clients for any loss of crypto-assets attributable to it.

Where *staking* services are provided in conjunction with any other crypto-asset services for which the Bank is authorised, the Bank must obtain the clients' explicit consent to *stake* their crypto-assets, as this may affect the clients' ability to access those assets.

k. Valuation of crypto-assets

[4] According to ESMA, in response to Q&A No. 2067.

Accurate valuation of crypto-assets is essential to ensure the correct assessment of the overall value of clients' portfolios, the custody fees to be charged and other associated charges, whilst guaranteeing transparency, fairness and alignment with the Bank's practices. The valuation method adopted for crypto-assets held in custody is carried out in the same way as for traditional financial assets at the Bank. It is based on valuations obtained from Bloomberg, which provides its proprietary Bloomberg Generic Price (BGN) – a composite calculated from quotes obtained from a carefully selected set of crypto-asset trading platforms that meet rigorous institutional standards.

I. Security systems applicable to the custody service

In the provision of the crypto-asset custody and management service, the Bank adopts security systems, procedures and mechanisms appropriate for the protection of clients' crypto-assets and the respective means of access, the operational implementation of which is detailed in points 3(d), 3(g) and 4(b)(ii) of this Policy.

5. Segregation of crypto-assets

a. Segregation of funds

As a credit institution authorised and registered with the Bank of Portugal, the Bank receives funds (banknotes, coins, book-entry fiat currency) from its clients. Accordingly, the Bank complies with all procedures relating to its activity as a credit institution, in particular with regard to payment services, current accounts and cash.

As Bison Bank is a credit institution, it is subject to prudential requirements, including those set out in the General Regime for Credit Institutions and Financial Companies ("RGICSF") – which transposes, amongst others, Directive 2013/36/EU (**"CRD** IV") and Directive 2014/59/EU ("BRRD") – Regulation (EU) No 575/2013 ("CRR") and Commission Delegated Regulation (EU) 2015/61, including those relating to liquidity management, leverage and asset risk, which aim to ensure the soundness of the institution and, consequently, the protection of its creditors, including depositors.

The prudential rules set out in the RGICSF, CRD IV, BRRD, CRR and other delegated regulations stipulate, amongst other things, that credit institutions must implement measures to ensure the maintenance of minimum own funds, leverage limits and sufficient liquidity to guarantee a robust and prudent financial position. Accordingly, Bison Bank is required to hold cash or high-quality liquid assets in sufficient quantities to cover its customers' claims.

In this way, customers will be safeguarded because Bison Bank will at all times maintain ratios that cover all its liabilities, including claims on funds deposited by customers with the Bank.

b. Segregation of crypto-assets

i. General principles

As with any asset the Bank holds in custody on behalf of its customers (including financial instruments, within the scope of its activity as a financial intermediary), the Bank segregates its customers' crypto-assets from its own assets, ensuring that the means of access to its customers' crypto-assets are clearly identified as such. To this end, the Bank segregates both the crypto- s held and the respective means of access, by holding them in global accounts ('jumbo accounts') with a computerised record of ownership by the relevant client.

The Bank maintains a register of clients' crypto-asset positions; these crypto-assets belong to the clients and do not form part of the Bank's assets or balance sheet. Consequently, in the event of the Bank's insolvency, clients' rights to their crypto-assets must be safeguarded, as they do not form part of the Bank's insolvency estate.

The Bank is expressly prohibited from carrying out any kind of proprietary trading with its clients' crypto-assets.

Segregation is primarily intended to protect clients' security, so that in the event of, for example, enforcement proceedings against the Bank or the Bank's insolvency, clients' crypto-assets are safeguarded and beyond the reach of the Bank's creditors in terms of assets to be pledged or seized for the insolvency estate. For this reason, crypto-assets held in custody are legally segregated from the Bank's assets, in the interests of clients, and any creditors of the Bank cannot satisfy any debts owed by the Bank using clients' crypto-assets held in custody by the Bank.

ii. *Wallets*

Crypto-assets held on behalf of clients are not, under any circumstances, used by the Bank for its own account. The Bank ensures, through its regular internal and audit processes, that all funds are held on a 1:1 basis by regularly verifying proof of funds in the various wallets under its management.

With regard to clients' crypto-assets, the Bank ensures that, in cases where these are held collectively in omnibus accounts ("jumbo accounts"), it is able to identify and account for the crypto-assets belonging to each client through its computerised records. To this end, the Bank has implemented a securities management system within its core system that enables it to identify the amount of assets belonging to each client and their location.

iii. System for the approval and safeguarding of cryptographic keys

The security of cryptographic keys is an essential element that has led the Bank to establish a comprehensive system for the approval and safeguarding of cryptographic keys, with a specific focus on MPC technology, with the aim of ensuring a high level of security and operational integrity.

With regard to the approval of cryptographic transactions, various transaction policies are in place based on asset, amount and type, always requiring approval from at least two operations managers.

As regards the safeguarding of cryptographic keys, these are split into fragments and stored on encrypted devices that are not connected to the internet and are kept in different geographical locations, so as to prevent their complete loss in the event of a security breach.

6. Approval and availability to clients

This Policy was approved by the Board of Directors on June 29, 2026 and takes effect immediately upon publication.

A summary of the custody policy must be made available to clients, upon their request, in electronic format.