

Diligência Devida do Cliente e Arcabouço de AML/Sanções v4.0.1

Alinhado com os T&C e com a Política de Privacidade | Data de Publicação (Publication Date): 24 de setembro de 2026

Este arcabouço de Diligência Devida do Cliente e AML/Sanções (o “Arcabouço”) constitui a versão canônica oficial em língua inglesa do arcabouço de diligência devida do cliente, de prevenção à lavagem de dinheiro e de conformidade com sanções adotado pela Neom Triple A Information Technology LLC, operando sob a marca NEOMAAA Funded. Este Arcabouço é publicado como compromisso voluntário com elevados padrões de proteção ao consumidor, prevenção a fraudes, conformidade com sanções e conduta empresarial ética, e é aplicado às atividades da Empresa como prestadora de serviços de avaliação por meio de operação simulada (simulated trading evaluation services). Este Arcabouço substitui todas as versões anteriormente publicadas da Política de AML / KYC da NEOMAAA Funded.

§1 Declaração do Arcabouço

1.1 A Neom Triple A Information Technology LLC (marca: NEOMAAA Funded, doravante a “Empresa”) assume um compromisso incondicional de cumprir todas as leis e regulamentos aplicáveis às suas atividades como prestadora de serviços de avaliação por operação simulada, incluindo obrigações de proteção ao consumidor, prevenção a fraudes, conformidade com sanções e conformidade tributária, e de observar, como boa prática voluntária e na medida aplicável, princípios derivados dos padrões internacionais de Prevenção à Lavagem de Dinheiro (Anti-Money Laundering, AML) e de Combate ao Financiamento do Terrorismo (Combating the Financing of Terrorism, CFT). Esse compromisso é fundamental para as operações lícitas da Empresa e para a manutenção da confiança de Participantes, parceiros bancários e reguladores.

1.2 A Empresa reconhece que suas atividades envolvendo o recebimento de pagamentos de Participantes no âmbito de programas de avaliação por operação simulada, bem como o desembolso de prêmios sob o Programa de Benefícios (Benefit Program) em conformidade com os T&C, comportam riscos de exploração em esquemas de lavagem de dinheiro ou de financiamento do terrorismo. Este Arcabouço estabelece medidas para identificar, avaliar e mitigar tais riscos.

1.3 Este Arcabouço aplica-se a todos os Participantes (conforme definido nos T&C §1.5(c)), a todos os empregados, diretores, contratados e agentes da Empresa, e a todas as operações financeiras vinculadas às atividades da Empresa. A Empresa implementa este Arcabouço por meio de uma abordagem baseada em risco (Risk-Based Approach, RBA), calibrando a intensidade das medidas de AML/CFT ao nível de risco identificado.

1.4 Este Arcabouço integra um conjunto documental composto pelos T&C, pela a Política de Privacidade e pela Política de Cookies. No caso de qualquer conflito entre este Arcabouço e os T&C, prevalecerão as disposições dos T&C.

§2 Escopo e Pessoa Jurídica

2.1 Pessoa Jurídica Controladora. Este Arcabouço aplica-se às operações da seguinte pessoa jurídica:

Nome legal completo: Neom Triple A Information Technology LLC Marca: NEOMAAA Funded
Endereço registrado: The Binary by Omniyat, Office 2114, Business Bay, Dubai, UAE Site: neomaaafunded.com

2.2 Escopo do Arcabouço. Este Arcabouço aplica-se:

1. a todos os Participantes, independentemente de sua jurisdição de residência ou cidadania;
2. a todas as transações de recebimento de pagamentos para Contas de Avaliação Financiada (§1.5(f) dos T&C) e Contas de Avaliação Expressa (§1.5(m) dos T&C), bem como a todos os desembolsos do Programa de Benefícios nos termos do §17 dos T&C;
3. a todos os empregados, diretores, contratados e representantes da Empresa;
4. a todos os terceiros que atuem em nome ou no interesse da Empresa em conexão com o recebimento ou desembolso de fundos.

2.3 Classificação da Atividade. A Empresa é prestadora de serviços de avaliação por operação simulada. A Empresa não é instituição financeira licenciada, instituição de crédito, corretora, dealer, consultora de investimentos ou prestadora de serviços de ativos virtuais na acepção de qualquer legislação aplicável, e não detém fundos, valores mobiliários ou investimentos de clientes. A Empresa observa o arcabouço abaixo como compromisso voluntário com elevados padrões de proteção ao consumidor, prevenção a fraudes e conformidade com sanções, independentemente de qualquer classificação de suas atividades nos termos do [UAE Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Financing of Illegal Organisations](#) ou da Cabinet Decision No. 134 of 2025.

2.4 Princípio do Padrão Mais Elevado. Quando exigências aplicáveis de diferentes jurisdições entrarem em conflito, a Empresa aplicará o padrão mais rigoroso compatível com as operações da Empresa enquanto pessoa jurídica constituída nos EAU.

§3 Arcabouço Regulatório

3.1 Arcabouço Regulatório dos EAU — Na Medida Aplicável. A Empresa observa os seguintes instrumentos regulatórios dos EAU como parte de seu arcabouço voluntário de AML/sanções, na medida aplicável às suas atividades:

1. [UAE Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations \(as superseded by Federal Decree-Law No. 10 of 2025\)](#) (doravante “UAE FDL 20/2018” ou “AML FDL”) — principal instrumento legislativo dos EAU que estabelece princípios de Diligência Devida do Cliente (Customer Due Diligence, CDD), Diligência Devida Reforçada (Enhanced Due Diligence, EDD), avaliação de atividade suspeita e manutenção de registros; observado pela Empresa como boa prática voluntária;
2. [Cabinet Decision No. 10 of 2019 concerning the Implementing Regulation of UAE Federal Decree-Law No. 20 of 2018](#) (substituída pela Cabinet Decision No. 134 of 2025, em vigor a partir de 14 de dezembro de 2025) — que estabelece requisitos procedimentais detalhados para identificação de clientes, gestão de riscos e reporte;
3. [UAE Federal Decree-Law No. 26 of 2021 amending certain provisions of Federal Decree-Law No. 20 of 2018](#) — que amplia a categoria de entidades obrigadas e reforça sanções;
4. [UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences](#) — que estabelece o conceito de financiamento do terrorismo e obrigações correlatas de contrafinanciamento;
5. [UAE Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes](#) — aplicável à dimensão digital das atividades da Empresa, incluindo sua plataforma online e transações

eletrônicas (este instrumento revogou e substituiu o UAE Federal Law No. 5 of 2012 com efeito a partir de 2 de janeiro de 2022);

6. [UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data](#) (a “UAE PDPL”) — que estabelece o arcabouço legal para o tratamento de dados pessoais nos EAU, incluindo as bases legais, os direitos do titular dos dados, as obrigações de segurança e os requisitos de transferência transfronteiriça aplicáveis ao tratamento, pela Empresa, de dados pessoais coletados, gerados ou retidos para fins de AML/CFT/CPF (incluindo CDD, EDD, monitoramento contínuo, documentação de SAER e período de manutenção de registros); e
7. [UAE Cabinet Decision No. 58 of 2020 on the Regulation of the Beneficial Owner Procedures](#) — que estabelece as obrigações de pessoas jurídicas nos EAU de identificar, registrar e reportar seus beneficiários efetivos, e fornece a definição operativa de Beneficiário Efetivo utilizada neste Arcabouço no §4.1.

3.2 Padrões Internacionais e Regimes de Sanções. Este Arcabouço também observa:

1. [Recomendações do Grupo de Ação Financeira Internacional \(Financial Action Task Force, FATF\)](#) — padrões internacionais para o combate à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação, em particular as Recomendações 1, 10, 11, 12, 15, 19 e 20;
2. [UN Security Council Consolidated List](#) — incluindo a lista consolidada de indivíduos, entidades e jurisdições sujeitos a sanções adotadas sob o Capítulo VII da Carta da ONU;
3. programas de sanções administrados pelo [U.S. Department of the Treasury Office of Foreign Assets Control \(OFAC\)](#), pela [União Europeia](#), pelo [HM Treasury \(United Kingdom\)](#) e pelo UAE Executive Office for AML/CFT.

3.3 Alterações no Cenário Regulatório. A Empresa monitora alterações na legislação aplicável e compromete-se a atualizar este Arcabouço com prontidão razoável após a entrada em vigor de qualquer emenda substancial. Em conformidade com §1.3(a)(iv) dos T&C, alterações exigidas por obrigações relacionadas a AML/CFT entram em vigor imediatamente após a publicação.

§4 Definições

4.1 Para os fins deste Arcabouço, aplicam-se as seguintes definições:

“Lavagem de Dinheiro” (Money Laundering) — atos definidos no [Artigo 2 do AML FDL](#): receber, adquirir, possuir, usar, transferir ou transformar fundos ou bens, quando a pessoa souber ou devesse saber que constituem produto de crime, com a intenção de ocultar ou dissimular sua origem ilícita, ou de auxiliar qualquer pessoa envolvida em um crime antecedente a evadir suas consequências legais.

“Financiamento do Terrorismo” (Financing of Terrorism) — a provisão ou coleta de fundos com a intenção, ou com a ciência, de que serão utilizados, no todo ou em parte, para financiar atividades nos termos da [UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences](#), ou para financiar indivíduos ou organizações engajados em atividades terroristas.

“Beneficiário Efetivo” (Ultimate Beneficial Owner, UBO) — a pessoa física que, em última instância, detém ou controla uma pessoa jurídica ou outra estrutura que seja cliente, ou a pessoa física em cujo nome uma transação é conduzida, em conformidade com a definição estabelecida na UAE Cabinet Decision No. 58 of 2020 on Beneficial Ownership Registers.

“Pessoa Politicamente Exposta” (Politically Exposed Person, PEP) — pessoa física que ocupa ou tenha ocupado uma função pública proeminente (chefe de Estado ou de governo, ministro de

governo, oficial militar sênior, diretor de empresa estatal, chefe de organização internacional, etc.), bem como membros próximos da família e associados próximos conhecidos dessa pessoa.

“Diligência Devida do Cliente” (Customer Due Diligence, CDD) — o conjunto de medidas padrão de identificação e verificação aplicadas em relação a um cliente, incluindo o estabelecimento da origem dos fundos, a avaliação da relação de negócios e sua finalidade.

“Diligência Devida Reforçada” (Enhanced Due Diligence, EDD) — medidas reforçadas de verificação aplicadas a clientes de maior risco, incluindo Pessoas Politicamente Expostas (PEPs), clientes de jurisdições de maior risco e outras pessoas especificadas no §7 deste Arcabouço.

“Diligência Devida Simplificada” (Simplified Due Diligence, SDD) — medidas reduzidas de verificação aplicadas a clientes de risco demonstradamente baixo, sujeitas à satisfação de todas as condições estabelecidas neste Arcabouço.

“Relatório de Escalonamento de Atividade Suspeita” (Suspicious Activity Escalation Report, SAER) — relatório interno escrito preparado por pessoal da Empresa, documentando indícios para suspeitar que uma transação ou conta esteja vinculada a lavagem de dinheiro, financiamento do terrorismo, fraude, evasão de sanções ou outra atividade ilícita, escalonado à Alta Administração para avaliação e qualquer providência adicional exigida pela lei aplicável.

“Responsável de Conformidade” (Head of Compliance) — o agente da Empresa responsável por coordenar os procedimentos de diligência devida do cliente, triagem de sanções e escalonamento interno de atividade suspeita estabelecidos neste Arcabouço.

“Participante” — pessoa física ou jurídica registrada para utilizar os Serviços da NEOMAAA Funded em conformidade com o §1.5(c) dos T&C.

“Conta de Avaliação Financiada” (Funded Evaluation Account) — conta simulada com saldo virtual fornecida a um Participante que tenha concluído com êxito a Fase de Avaliação, na aceção do §1.5(f) dos T&C.

“Conta de Avaliação Expressa” (Express Evaluation Account) — Conta de Avaliação Financiada de fase única, conforme previsto no §1.5(m) dos T&C.

“Nível de Reconhecimento” (Recognition Level) — parâmetro contratual selecionado pelo Participante na aquisição de uma Conta de Avaliação Financiada, que determina o Coeficiente de Recompensa e o Capital Simulado Inicial, na aceção do §1.5(y) dos T&C.

§5 Abordagem Baseada em Risco

5.1 Princípio da Proporcionalidade. Em conformidade com a [Recomendação 1 do FATF](#) e com o [AML FDL](#), a Empresa aplica medidas de Diligência Devida do Cliente (CDD), Diligência Devida Reforçada (EDD) e de monitoramento proporcionais ao nível de risco identificado. A intensidade das medidas é estabelecida de forma proporcional ao risco e não é aplicada uniformemente a todos os clientes.

5.2 Fatores de Avaliação de Risco. A Empresa avalia os seguintes fatores de risco em relação a cada Participante e à relação de negócios com esse Participante:

1. Risco do Cliente: tipo de cliente (pessoa física, pessoa jurídica, estrutura corporativa), ocupação, condição de Pessoa Politicamente Exposta (PEP) ou vinculação a PEP, histórico de estornos (chargebacks) ou disputas de pagamento, conduta durante o KYC.
2. Risco Geográfico: país de residência e de cidadania do Participante, país da origem dos fundos, consistência do endereço IP com os dados de KYC, classificação da jurisdição segundo as listas do FATF, as listas de Países Terceiros de Alto Risco da UE ou as listas de sanções aplicáveis.

3. Risco de Produto: tipo de conta utilizada (Conta de Avaliação Financiada, Conta de Avaliação Expressa), montantes agregados de pagamentos e desembolsos do Programa de Benefícios, frequência e padrão de transações, Nível de Reconhecimento selecionado.
4. Risco de Canal: natureza da interação (remota/não presencial), uso de ferramentas de anonimização (VPN, proxy, Tor) em violação ao §7.10.1(l) dos T&C, discrepância entre o endereço IP e a jurisdição declarada no KYC.

5.3 Níveis de Diligência Devida. Com base na avaliação agregada dos fatores de risco, a Empresa aplica um de três níveis de diligência devida:

1. Diligência Devida Padrão do Cliente (Standard CDD) — para Participantes com nível de risco baixo ou moderado. Inclui verificação de identidade por meio da Sumsub, triagem contra listas de sanções e listas de PEPs, e avaliação da origem dos fundos.
2. Diligência Devida Reforçada (EDD) — para Participantes de maior risco. Aplicada nas circunstâncias especificadas no §7 deste Arcabouço. Inclui documentação adicional, declaração de origem do patrimônio e aprovação da alta administração.
3. Diligência Devida Simplificada (SDD) — aplicada exclusivamente em relação a pessoas jurídicas listadas em bolsas reguladas em jurisdições com regime de AML adequado, e a órgãos governamentais, na ausência de quaisquer indicadores de risco.

5.4 Documentação. A avaliação de risco de cada Participante é documentada no arquivo do cliente. Qualquer alteração manual (override) de uma avaliação de risco requer justificativa por escrito e aprovação do Responsável de Conformidade da Empresa.

5.5 Revisão da Avaliação de Risco. A avaliação de risco de cada Participante é revisada na ocorrência de qualquer dos seguintes eventos: qualquer alteração substancial no volume ou comportamento das transações; solicitação de desembolso do Programa de Benefícios; identificação de sinais de alerta (red flags); e, em qualquer caso, não menos do que uma vez por ano para Participantes de maior risco.

§6 Diligência Devida do Cliente (CDD)

6.1 Gatilhos de KYC. A Empresa realiza ou atualiza a verificação de Conheça Seu Cliente (Know Your Customer, KYC) nas seguintes circunstâncias:

1. na abertura de nova conta ou no primeiro pagamento referente a qualquer tipo de Conta Prop;
2. na primeira solicitação de desembolso do Programa de Benefícios;
3. [Reservado intencionalmente];
4. na identificação de atividade incomum, sinais de alerta ou alteração no perfil de risco do Participante;
5. em solicitação dirigida ao Participante nos termos do §7.10.1(m) dos T&C em conexão com possível envolvimento de terceiros;
6. na revisão periódica programada do arquivo do cliente (Participantes de maior risco: a cada 6 meses; risco médio: a cada 12 meses; risco menor: a cada 36 meses).

6.2 Dados Coletados. Como parte da Diligência Devida do Cliente (CDD) padrão, a Empresa coleta os seguintes dados e documentos:

1. documento de identidade: passaporte válido (página de foto e de dados biográficos), carteira de identidade nacional da UE, ou carteira de motorista (em jurisdições nas quais seja aceita como documento de identificação satisfatório);

2. verificação biométrica por selfie: gravação de vídeo dinâmica (liveness check) ou selfie estática com o documento de identidade, para impedir o uso de documentos de terceiros e contas com deepfake;
3. comprovante de endereço residencial: fatura de serviço público, extrato bancário, correspondência oficial de governo ou contrato de locação, emitido em até três meses antes da entrega;
4. Declaração de Origem dos Fundos: obrigatória quando o volume agregado de pagamentos ou desembolsos exceder os limiares estabelecidos pela Empresa (limiares específicos não são divulgados nesta versão pública do Arcabouço, em conformidade com os princípios de confidencialidade dos controles de AML da Empresa).

6.3 Provedor de KYC/IDV. A Empresa realiza a verificação de identidade e as verificações biométricas por meio da plataforma Sumsb (Sum and Substance Ltd / Sumsb Group). A Sumsb é o provedor de KYC/AML da Empresa, referido na categoria de destinatários (ii) do §6 da Política de Privacidade. Os dados pessoais são transferidos para a Sumsb sob um acordo escrito de tratamento de dados que incorpora Cláusulas Contratuais Padrão (Standard Contractual Clauses, SCCs) em conformidade com a [Commission Implementing Decision \(EU\) 2021/914](#). Uma lista completa dos atuais provedores de KYC/IDV está disponível mediante solicitação em privacy@neomaaafunded.com.

6.4 Triagem em Tempo Real de PEP e de Sanções. Por ocasião do KYC, cada Participante é submetido a:

1. triagem em tempo real contra as listas atuais de Pessoas Politicamente Expostas (PEPs) (Dow Jones Risk & Compliance, WorldCheck ou bases de dados equivalentes integradas por meio da Sumsb);
2. triagem contra as listas de sanções estabelecidas no §9 deste Arcabouço;
3. triagem de mídia adversa contra bases de dados relevantes.

A triagem é realizada tanto na incorporação (onboarding) quanto de forma contínua. Quando uma correspondência ou possível correspondência for identificada, aplica-se o procedimento descrito no §9 deste Arcabouço.

6.5 Verificação de Número de Telefone. Em conformidade com o §6.1 dos T&C, exige-se que o Participante conclua a verificação do número de telefone por código SMS no prazo de sete (7) dias corridos a contar do primeiro pagamento ou do registro da conta. A falta de verificação resulta em acesso restrito a recursos da plataforma, incluindo a criação de novas contas e solicitações de desembolso do Programa de Benefícios.

6.6 Contas de Sorteio. Participantes que tenham recebido contas por meio de sorteios (giveaways), promoções de premiação ou ofertas de parceiros devem concluir a verificação completa de KYC antes que qualquer solicitação de desembolso do Programa de Benefícios seja processada, em conformidade com o §7.12(B)(v) dos T&C.

6.7 Clientes Corporativos. Quando uma pessoa jurídica realiza registro, a Empresa solicita adicionalmente: certificado de constituição, Memorandum of Association, documentos confirmando a autoridade do representante autorizado e documentos da estrutura societária que revelem todos os Beneficiários Finais (UBOs) detentores de mais de 25% das ações ou direitos de voto (em conformidade com a UAE Cabinet Decision No. 58 of 2020). Estruturas nas quais o beneficiário efetivo não puder ser identificado não são aceitas para atendimento.

6.8 Consequências do Descumprimento do KYC. Em conformidade com os §6.4 dos T&C e §6.4.2 dos T&C, a falta de conclusão da verificação de KYC pelo Participante resultará em acesso restrito aos Serviços e poderá resultar em rescisão em conformidade com o §15 dos T&C.

§7 Diligência Devida Reforçada (EDD)

7.1 Gatilhos Obrigatórios de EDD. A Diligência Devida Reforçada (EDD) é obrigatória nas seguintes circunstâncias:

1. condição de PEP identificada ou suspeita: o Participante é Pessoa Politicamente Exposta (PEP), membro da família de PEP ou associado próximo conhecido de PEP;
2. o Participante é residente ou cidadão de jurisdição incluída na lista “Call for Action” do FATF ou na lista da Comissão Europeia de países terceiros de alto risco;
3. tiver sido identificada conexão ou possível conexão com pessoa ou entidade sancionada;
4. tiver sido identificado padrão de transação incomum: estruturação de pagamentos, retirada imediata de fundos após o recebimento, pagamentos com dados de pagamento que não correspondam às informações verificadas do Participante;
5. discrepância entre o endereço IP ou a geolocalização e a jurisdição declarada, em conformidade com §7.10.1(I) dos T&C;
6. valor agregado elevado de desembolsos do Programa de Benefícios para um único Participante;
7. identificação de coordenação de atividade de operação entre múltiplas contas em conformidade com o §7.12 dos T&C;
8. qualquer outro fator que indique nível mais elevado de risco no julgamento do Responsável de Conformidade.

7.2 Medidas Adicionais de EDD. A Diligência Devida Reforçada (EDD) inclui as seguintes medidas adicionais, além da Diligência Devida do Cliente (CDD) padrão:

1. obtenção de aprovação da alta administração antes do início ou da continuidade de relação de negócios com Participante sujeito a EDD;
2. obtenção de Declaração de Origem do Patrimônio (Source of Wealth Declaration) com evidência documental comprobatória (declarações fiscais, contrato de trabalho, documentos de transação imobiliária, etc.);
3. obtenção de Declaração detalhada de Origem dos Fundos para cada transação substancial;
4. verificação de documentos por meio de fontes independentes adicionais;
5. monitoramento contínuo reforçado da relação de negócios com o Participante;
6. ciclo abreviado de revisão periódica do arquivo do cliente (a cada seis (6) meses, em vez dos 12 ou 36 meses padrão).

7.3 Documentação da EDD. Todas as medidas de Diligência Devida Reforçada (EDD) são documentadas no arquivo do cliente, registrando: a data em que a EDD foi conduzida; os fundamentos para a aplicação da EDD; os resultados de cada medida; o nome do agente que conduziu a EDD; e a decisão alcançada após a EDD, com a assinatura do Responsável de Conformidade.

7.4 Proibição de Atendimento Sem Conclusão da EDD. Todos os desembolsos do Programa de Benefícios ficam suspensos até a conclusão do procedimento de EDD e decisão favorável do Responsável de Conformidade. Essa suspensão não constitui descumprimento das obrigações da Empresa para com o Participante.

§8 Jurisdições Proibidas

8.1 Proibição Absoluta. A Empresa não presta Serviços a Participantes que sejam residentes, cidadãos de, ou atuem em nome das seguintes jurisdições sujeitas a sanções abrangentes ou classificadas pelo FATF como “Call for Action”:

1. Cuba;
2. Irã;
3. República Popular Democrática da Coreia (RPDC / Coreia do Norte);
4. Mianmar (na medida coberta pela lista FATF Call for Action);
5. Síria;
6. Rússia;
7. Venezuela;
8. territórios sujeitos a regimes de sanções abrangentes na Data de Vigência: Crimeia, República Popular de Donetsk, República Popular de Lugansk, Oblast de Zaporíjia, Oblast de Kherson (territórios anexados/ocupados da Ucrânia sob sanções do OFAC, da UE e da ONU);
9. Belarus;
10. Líbia, Sudão, Somália, Iraque, Iêmen, Mali, Líbano — na medida exigida pelos regimes de sanções aplicáveis da ONU, da UE, do OFAC e do UK HMT;
11. qualquer outro país ou território sujeito a sanções abrangentes administradas pelo [UN Security Council](#), pela [União Europeia](#), pelo [OFAC](#) ou pelo [HM Treasury](#).

8.2 Lista Cinza do FATF — Precauções Reforçadas. Em relação a Participantes oriundos de jurisdições incluídas na lista “Jurisdictions under Increased Monitoring” do FATF (lista cinza), a Diligência Devida Reforçada (EDD) obrigatória aplica-se em conformidade com o §7 deste Arcabouço. A inclusão na lista cinza do FATF não constitui, por si só, fundamento para recusa automática de Serviços, desde que a EDD seja concluída com êxito. A lista atual é publicada no site oficial do FATF: <https://www.fatf-gafi.org/>.

8.3 Restrições Adicionais Impostas pela Empresa. Em conformidade com o §7.17 dos T&C, a Empresa também não presta Serviços nas seguintes jurisdições por motivos comerciais ou regulatórios: Estados Unidos da América — salvo quando expressamente permitido pela Empresa em conformidade com a legislação estadual aplicável; Canadá — salvo quando expressamente permitido pela Empresa. A lista completa e atualizada de jurisdições restritas está estabelecida no §7.17 dos T&C, publicado em neomaaafunded.com.

8.4 Responsabilidade do Participante. Em conformidade com o §7.17(d) dos T&C, o Participante é o único responsável pelo cumprimento das leis aplicáveis de sua jurisdição. O registro ou o uso dos Serviços a partir de jurisdição proibida constitui descumprimento substancial dos T&C e resultará na suspensão imediata da conta, sem aviso prévio, em conformidade com o §7.17(d) dos T&C.

8.5 Monitoramento e Atualizações. A Empresa mantém monitoramento contínuo de desenvolvimentos em sanções e regulação e atualiza a lista de jurisdições proibidas a cada alteração nos regimes de sanções da ONU, da UE, do OFAC e do HM Treasury, bem como após cada sessão plenária do FATF (não menos do que três vezes por ano).

§9 Triagem de Sanções

9.1 Listas de Sanções Aplicáveis. A Empresa realiza triagem de todos os Participantes contra as seguintes listas:

1. [UN Security Council Consolidated List](#) — todas as resoluções de sanções adotadas sob o Capítulo VII da Carta da ONU;
2. [EU Consolidated Sanctions List](#);
3. [OFAC SDN List \(Specially Designated Nationals and Blocked Persons List\)](#), juntamente com a OFAC Sectoral Sanctions Identifications (SSI);
4. [UK OFSI Consolidated List \(HM Treasury Financial Sanctions Consolidated List\)](#);
5. UAE Local Terrorist List, juntamente com as listas de sanções administradas pelo UAE Executive Office for AML/CFT.

9.2 Triagem de PEP. A triagem de condição de Pessoa Politicamente Exposta (PEP) é realizada utilizando Dow Jones Risk & Compliance, WorldCheck ou bases de dados equivalentes integradas à plataforma Sumsb, bem como por meio de fontes públicas: registros oficiais de governo, bases de dados de organizações internacionais e publicações na mídia.

9.3 Frequência da Triagem. A triagem é realizada:

1. em toda incorporação (onboarding) de novo Participante, antes da provisão de acesso aos Serviços;
2. a cada atualização das listas de sanções aplicáveis;
3. antes de cada desembolso do Programa de Benefícios;
4. a qualquer alteração nos dados pessoais do Participante;
5. ao acréscimo de novo método de pagamento ou dados de saque.

9.4 Procedimento Mediante Identificação de Correspondência de Sanções. Quando uma correspondência ou possível correspondência com qualquer lista de sanções aplicável for identificada:

1. a transação e a conta são imediatamente congeladas, sem notificação ao Participante;
2. o Responsável de Conformidade analisa a correspondência no prazo de 24 horas para determinar se é correspondência verdadeira ou falso positivo;
3. quando o resultado for falso positivo: a constatação é registrada no arquivo do cliente com justificativa por escrito;
4. quando confirmada correspondência verdadeira: os fundos permanecem congelados; um relatório é submetido à autoridade de sanções competente no prazo legalmente prescrito; nenhum descongelamento é efetuado sem a autorização expressa por escrito da autoridade de sanções competente; o Responsável de Conformidade notifica a Alta Administração.

9.5 Proibição. É estritamente proibido descongelar os fundos de pessoa sancionada sem a autorização escrita da autoridade de sanções competente (OFAC, UE ou autoridade competente pertinente).

§10 Monitoramento de Transações

10.1 Sistema de Monitoramento. A Empresa opera um sistema multicamadas de monitoramento de transações que combina análise automatizada com revisão manual por membros da equipe de conformidade.

10.2 Gatilhos Automatizados. O sistema de monitoramento gera alertas ao identificar, entre outros, os seguintes padrões:

1. Estruturação: padrão de pagamentos estruturados de modo a permanecer abaixo de limiares estabelecidos ou a evitar requisitos de verificação.
2. Entrada/saída rápida (rapid in/out): movimentação imediata de fundos após seu recebimento, sem qualquer propósito econômico aparente.
3. Incompatibilidade geográfica: transações de pagamento originárias de jurisdições incompatíveis com os dados de KYC do Participante.
4. Pagamentos por terceiros: recebimento de fundos de pessoas que não sejam o titular verificado da conta, ou solicitações de saque para dados que não pertençam ao Participante.
5. [Reservado intencionalmente];
6. Dados de pagamento compartilhados entre contas diferentes: métodos de pagamento comuns ou destinos de saque compartilhados entre contas diferentes, em conformidade com o §7.12(C)(vi) dos T&C.
7. Uso de ferramentas de anonimização: uso de VPN, Tor ou serviços de proxy em violação ao §7.10.1(l) dos T&C.

10.3 Monitoramento Comportamental da Atividade de Operação. Em adição ao monitoramento de transações, a Empresa conduz monitoramento comportamental da atividade de operação dos Participantes para identificar padrões que possam indicar conduta coordenada ou fraudulenta com significado para AML: operações casadas (matched trades), operação em grupo / atividade coordenada, compartilhamento de contas e inconsistências de IP/geolocalização em conformidade com o §7.10.1(l) e (m) dos T&C.

10.4 Limiares. Limiares numéricos específicos de monitoramento de transações não são divulgados nesta versão pública do Arcabouço, a fim de preservar a confidencialidade dos controles de AML da Empresa. Os gatilhos são aplicados de forma combinada: limiar E comportamental.

10.5 Revisão Manual. Todos os alertas do sistema de monitoramento ficam sujeitos a revisão manual por membro autorizado da equipe de conformidade. Indicadores não justificados por fundamentos legítimos são escalonados ao Responsável de Conformidade para avaliação quanto à necessidade de preparar um Relatório de Escalonamento de Atividade Suspeita (SAER) em conformidade com o §11 deste Arcabouço.

10.6 Sinais de Alerta Típicos. Sinais de alerta (red flags) que requerem atenção imediata da equipe de conformidade incluem, entre outros:

- recusa de um Participante em fornecer documentação de KYC sem explicação razoável;
- documentos com sinais de alteração ou inconsistência;
- preocupação excessiva por parte de um Participante quanto a procedimentos de monitoramento;
- perfil transacional substancialmente inconsistente com a origem dos fundos declarada;
- o endereço IP do Participante no login não corresponde à jurisdição declarada no KYC;
- operações de mirror-trading entre contas seguidas de desembolsos do Programa de Benefícios para ambas as contas;
- estornos (chargebacks) repetidos ou disputas de pagamento seguidos de novo aporte na conta.

§11 Escalonamento Interno de Atividade Suspeita

11.1 Definição. Considera-se que uma transação ou conta dá margem a fundamentos de atividade suspeita quando a Empresa tem ciência, suspeita ou fundamentos razoáveis para suspeitar de que a transação ou os fundos estão vinculados a atividade criminosa, lavagem de dinheiro, financiamento do terrorismo, evasão de sanções ou fraude, independentemente do valor da transação. Quando a Empresa posteriormente determinar que surge alguma obrigação de reporte externo nos termos da lei aplicável, a Empresa cumprirá tal obrigação em conformidade com os procedimentos da autoridade competente.

11.2 Responsabilidades do Responsável de Conformidade. O Responsável de Conformidade da Empresa é o único responsável por:

1. receber divulgações internas de atividade suspeita feitas por empregados da Empresa;
2. avaliar cada divulgação interna e preparar um Relatório de Escalonamento de Atividade Suspeita (SAER) para a Alta Administração, quando o escalonamento for justificado;
3. avaliar se surge qualquer obrigação de reporte externo nos termos da lei aplicável e, quando tal obrigação surgir, cumpri-la em conformidade com os procedimentos da autoridade competente;
4. documentar todas as decisões, inclusive decisões de não escalonar ou de não realizar qualquer reporte externo, com justificativa por escrito.

11.3 Processo de Escalonamento Interno.

Etapa 1 — Detecção: um empregado ou sistema automatizado identifica um ou mais sinais de alerta.

Etapa 2 — Escalonamento: dentro do prazo prescrito pelos procedimentos internos, o empregado apresenta ao Responsável de Conformidade uma divulgação interna escrita de atividade suspeita descrevendo os sinais de alerta identificados e as medidas já adotadas.

Etapa 3 — Revisão de Conformidade: o Responsável de Conformidade revisa o material apresentado. Quando necessário, o Responsável de Conformidade solicita informações adicionais aos empregados ou ao provedor Sumsub.

Etapa 4 — Decisão: o Responsável de Conformidade toma uma de duas decisões: preparar um Relatório de Escalonamento de Atividade Suspeita (SAER) para a Alta Administração ou recusar-se a fazê-lo, com justificativa por escrito.

Etapa 5 — Escalonamento e reporte externo (se aplicável): o Responsável de Conformidade escalona o Relatório de Escalonamento de Atividade Suspeita (SAER) à Alta Administração e avalia se surge alguma obrigação de reporte externo nos termos da lei aplicável. Quando tal obrigação surgir, o Responsável de Conformidade assegura o cumprimento tempestivo em conformidade com os procedimentos da autoridade competente.

Etapa 6 — Documentação: todo o processo é documentado. Relatórios internos e correspondência são retidos por, no mínimo, cinco (5) anos em conformidade com o §12 deste Arcabouço.

11.4 Prazos. Um Relatório de Escalonamento de Atividade Suspeita (SAER) é preparado e escalonado à Alta Administração sem atraso indevido a partir do momento em que o pessoal da Empresa souber, suspeitar ou tiver fundamentos razoáveis para suspeitar de fundamentos para escalonamento. Qualquer obrigação de reporte externo decorrente de lei aplicável é cumprida dentro do prazo prescrito por essa lei.

11.5 Tipping-Off (Vazamento). A Empresa observa a proibição de tipping-off refletida no Artigo 25 do [UAE Federal Decree-Law No. 10 of 2025](#) como boa prática voluntária. A Empresa, seus empregados, diretores e agentes abster-se-ão de divulgar ao Participante ou a qualquer terceiro o

fato de que ocorreu escalonamento interno de atividade suspeita, ou de que qualquer reporte externo foi ou poderá ser feito, ou de que uma investigação está sendo conduzida em conexão com suspeitas de lavagem de dinheiro, financiamento do terrorismo, fraude ou evasão de sanções, salvo quando tal divulgação for exigida pela lei aplicável.

11.6 Congelamento de Ativos Mediante Atividade Suspeita. Mediante a preparação de um Relatório de Escalonamento de Atividade Suspeita (SAER) ou a identificação de correspondência de sanções, a Empresa poderá congelar a conta do Participante e suspender todos os desembolsos do Programa de Benefícios. Esse congelamento não constitui descumprimento das obrigações da Empresa para com o Participante; quaisquer atrasos em desembolsos decorrentes de requisitos legais de AML ou de sanções não dão margem a responsabilidade por parte da Empresa, em conformidade com o §1.5(t)(v) dos T&C.

§12 Manutenção de Registros

12.1 Princípio Geral. Em conformidade com o [Artigo 16\(1\)\(f\) do AML FDL](#) e com as [Recomendações do Financial Action Task Force \(FATF\)](#) (Recomendação 11), a Empresa retém todos os documentos e registros relativos às relações de negócios com Participantes e a todas as transações pelo período mínimo de cinco (5) anos a contar do término da relação de negócios ou da data da transação. Esse período de retenção é consistente com o §8(a) da Política de Privacidade.

12.2 Registros Sujeitos a Retenção. Os seguintes registros estão sujeitos a retenção obrigatória, incluindo:

1. documentos de identidade (KYC/CDD): passaportes, carteiras de identidade, comprovantes de endereço, resultados de verificação da Sumsb, capturas de tela das verificações biométricas e resultados de triagem de condição de PEP;
2. documentos de EDD: declarações de Origem dos Fundos (Source of Funds, SOF) e de Origem do Patrimônio (Source of Wealth, SOW), evidências documentais de origem dos fundos e decisões de aprovação de EDD pela alta administração;
3. registros de transações: histórico de pagamentos, histórico de desembolsos do Programa de Benefícios e logs de processamento de pagamentos;
4. registros de triagem de sanções: resultados de triagem automatizada e manual em relação a cada Participante e a cada transação, incluindo anotações de correspondências, possíveis correspondências e sua resolução;
5. Relatórios internos de Escalonamento de Atividade Suspeita (SAERs) e correspondência de investigação de conformidade;
6. quaisquer reportes externos feitos a autoridades competentes nos termos da lei aplicável, quando tal obrigação tiver surgido, e recibos confirmando sua apresentação;
7. registros de revisões periódicas dos arquivos de clientes;
8. registros de correspondência com Participantes relativos a procedimentos de KYC/AML.

12.3 Requisitos Técnicos de Armazenamento. Todos os registros são armazenados em formato seguro (criptografia AES-256 em repouso, TLS 1.2 ou superior em trânsito) em conformidade com o §29.9 dos T&C. Os registros devem ser acessíveis às autoridades regulatórias e à UAE FIU mediante a primeira solicitação. A destruição antecipada de registros antes do término do período de retenção aplicável é proibida. Mediante o recebimento de solicitação de regulador ou da UAE FIU, o período de retenção fica suspenso até a conclusão dos respectivos procedimentos.

12.4 Período de Retenção Estendido. Quando estiverem em curso procedimentos judiciais, regulatórios ou de AML em relação a um Participante, o período de retenção dos registros pertinentes fica estendido até a conclusão desses procedimentos mais um (1) ano.

12.5 Resumo dos Períodos de Retenção:

- Registros de KYC/AML: mínimo de 5 anos a contar do término da relação de negócios ou da data da transação (UAE FDL 20/2018 + Recomendação 11 do FATF)
- Registros de transações: mínimo de 7 anos
- Registros de SAER e quaisquer reportes externos: mínimo de 5 anos após sua preparação ou apresentação

§13 Treinamento e Conscientização

13.1 Treinamento Anual Obrigatório. Em conformidade com os requisitos do AML FDL e das melhores práticas internacionais, todos os empregados da Empresa com acesso a dados de clientes, operações de pagamento ou procedimentos de AML/CFT são obrigados a concluir treinamento de AML/CFT/CPF anualmente.

13.2 Programa de Treinamento. O programa de treinamento obrigatório abrange, entre outros temas:

1. o arcabouço regulatório de AML/CFT/CPF (o AML FDL, a UAE Cabinet Decision No. 134 of 2025, as Recomendações do Financial Action Task Force (FATF));
2. tipologias de lavagem de dinheiro e de financiamento do terrorismo características do setor de prop-trading;
3. os procedimentos de KYC/CDD/EDD da Empresa;
4. sinais de alerta e procedimentos de escalonamento;
5. conformidade com sanções e procedimentos de triagem;
6. a proibição de tipping-off (quando aplicável) e os procedimentos de Relatório de Escalonamento de Atividade Suspeita (SAER), incluindo a avaliação de quaisquer obrigações de reporte externo nos termos da lei aplicável;
7. canais internos de denúncia (whistleblowing);
8. atualizações na legislação aplicável e na prática regulatória.

13.3 Treinamento Especializado. A equipe de Conformidade e o Responsável de Conformidade passam por programa estendido de treinamento especializado, incluindo treinamento no uso da plataforma Sumsb, na interpretação de resultados de triagem de sanções e na avaliação de quaisquer obrigações de reporte externo decorrentes da lei aplicável.

13.4 Documentação do Treinamento. Todas as sessões de treinamento são documentadas (data, participantes, conteúdo programático, duração). Os registros de treinamento são retidos por, no mínimo, cinco (5) anos. O Responsável de Conformidade mantém um registro da conclusão do treinamento de cada empregado.

13.5 Novos Empregados. Os novos empregados são obrigados a concluir treinamento introdutório de AML/CFT no prazo de trinta (30) dias da data de sua admissão.

§14 Governança e Contatos

14.1 Estrutura de Governança de Conformidade. A Empresa estabeleceu a seguinte estrutura de governança:

1. Responsável de Conformidade: coordena os procedimentos de diligência devida do cliente, triagem de sanções e escalonamento de atividade suspeita estabelecidos neste Arcabouço; recebe e avalia divulgações internas de atividade suspeita; prepara Relatórios de Escalonamento de Atividade Suspeita (SAERs) para a Alta Administração; avalia se surge qualquer obrigação de reporte externo nos termos da lei aplicável e assegura o respectivo cumprimento; organiza o treinamento de pessoal e as revisões independentes.
2. Alta Administração: aprova este Arcabouço e quaisquer alterações; aprova a incorporação (onboarding) de Participantes de maior risco (EDD); recebe o relatório anual do Responsável de Conformidade sobre a efetividade do Arcabouço.
3. Conselho de Administração: recebe os resultados da revisão anual independente deste Arcabouço diretamente do revisor; tem a responsabilidade última pelo adequado funcionamento do programa de conformidade da Empresa.

Cadeia de responsabilização: Responsável de Conformidade → Alta Administração → Conselho de Administração.

14.2 Revisão Anual Independente. A Empresa contrata uma revisão externa independente deste Arcabouço, no mínimo, uma vez por ano. O revisor deverá ser independente da administração operacional da Empresa e deverá possuir competência demonstrada em diligência devida do cliente, conformidade com AML/sanções e proteção ao consumidor. Os resultados da revisão são reportados diretamente ao Conselho de Administração. O Responsável de Conformidade deverá elaborar plano de remediação para as deficiências identificadas no prazo de trinta (30) dias a contar do recebimento do relatório de revisão.

14.3 Revisão Anual do Arcabouço. Este Arcabouço é revisado, no mínimo, uma vez por ano, e a cada alteração substancial na legislação aplicável ou no modelo de negócios da Empresa.

14.4 Proteção ao Denunciante. Empregados da Empresa que, de boa-fé, reportem transações suspeitas ou descumprimentos de conformidade interna ou externamente à autoridade competente estão protegidos contra todas as formas de retaliação, ação adversa e discriminação, em conformidade com a lei aplicável dos EAU.

14.5 Dados de Contato. Para todas as consultas relativas a este Arcabouço, aos procedimentos de diligência devida do cliente ou à conformidade com sanções, os Participantes e demais interessados poderão entrar em contato:

Consultas sobre diligência devida do cliente, sanções e conformidade:
compliance@neomaaafunded.com

Consultas gerais e suporte: support@neomaaafunded.com

Endereço registrado: Neom Triple A Information Technology LLC The Binary by Omniyat, Office 2114 Business Bay, Dubai, UAE

Site: neomaaafunded.com

14.6 Alterações ao Arcabouço. A Empresa reserva-se o direito de alterar este Arcabouço a qualquer momento. A versão atual do Arcabouço é publicada em neomaaafunded.com. Alterações substanciais entram em vigor em conformidade com o procedimento estabelecido no §1.3 dos T&C.

Este Arcabouço de Diligência Devida do Cliente e AML/Sanções entra em vigor em 24 de setembro de 2026. Este Arcabouço substitui todas as versões anteriores da Política de AML / KYC ou documento equivalente publicado pela Neom Triple A Information Technology LLC sob a marca NEOMAAA Funded.

Arcabouço de Diligência Devida do Cliente e AML/Sanções v4.0.1 | Neom Triple A Information Technology LLC (NEOMAAA Funded) | Data de Publicação: 24 de setembro de 2026