MAUD CAPITAL GESTORA DE ATIVOS LTDA.

(“Maud”)

Manual de Controles Internos
(*Compliance*)

JANEIRO 2024

I. INTRODUÇÃO E GOVERNANÇA

1.1. O Manual de Controles Internos da Maud ("Manual") prescreve orientações gerais e define as regras que devem ser seguidas para a gestão adequada dos controles internos e os riscos operacionais na gestora. O objetivo deste Manual é auxiliar todos os Colaboradores (conforme definição abaixo) a compreenderem os requisitos legais e regulamentares aplicáveis ao contexto das atividades desenvolvidas pela Maud, bem como levar ao conhecimento dos Colaboradores (conforme definição abaixo) os métodos, controles e normas de conduta internos aos quais todos devem aderir.

1.2. Este Manual não é exaustivo e está sujeito a mudanças, correções, atualizações e revisões contínuas. Este Manual deve ser lido em conjunto com o Código de Ética e Conduta da Maud, o qual também contém regras atinentes aos objetivos aqui descritos.

1.3. Este Manual está de acordo com a regulamentação aplicável, o que inclui mas não se limita ao Código ANBIMA de Administração de Recursos de Terceiros e a regulamentação vigente emitida pela Comissão de Valores Mobiliários ("CVM").

1.4. Caso surja alguma situação não prevista neste Manual ou quaisquer dúvidas e/ou necessidade de esclarecimento quanto ao conteúdo deste Manual, o Colaborador deve buscar auxílio junto à área de *Compliance* da Maud por meio do e-mail: vobara@maud.capital.

II. GOVERNANÇA

2.1. As regras e procedimentos aqui definidos visam ao atendimento das leis, normas, regulamentações e políticas aplicáveis à Maud, e pretendem disseminar os procedimentos de controles internos. A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor estatutário responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Maud nos termos da Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21") ("Diretor de *Compliance*").

2.2. Nos termos do art. 25 da Resolução CVM 21, o Diretor de *Compliance* é o diretor responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos neste Manual.

2.3. O Diretor de *Compliance* exerce suas funções com plena independência e não atua em funções que possam afetar sua isenção, dentro ou fora da Maud. Da mesma forma, a área de *Riscos e Compliance* não está sujeita a qualquer ingerência por parte de outras áreas e possui autonomia para questionar os riscos assumidos nas operações realizadas pela Maud.

2.4. Deve ser garantido à área de *Riscos e Compliance* amplo acesso às informações e documentos relacionados às atividades da Maud, de modo que se possa verificar continuamente a conformidade com a legislação e as regras internas.

2.5. O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual. Caso o Diretor de *Compliance* tenha que se ausentar por mais de 30 (trinta) dias, o Comitê de *Riscos e Compliance* deverá designar um substituto ou um responsável temporário para cumprir suas funções durante este período de ausência.

2.6. O Diretor de *Compliance* tem como principais atribuições e responsabilidades: (i) o suporte a todas as áreas da Maud no que concerne aos esclarecimentos de controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Maud com as normas regulamentares (internas e externas) em vigor; e (ii) a definição, junto ao Comitê de *Riscos e Compliance*, dos planos de ação, seguida do monitoramento do cumprimento dos prazos e do nível de excelência dos trabalhos efetuados, assegurando que quaisquer desvios identificados possam ser prontamente corrigidos.

2.7. São outras atribuições do Diretor de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*: (i) assegurar o cumprimento da lei e de todas as normas e regulamentos (internos ou externos) que regem as atividades da Maud; (ii) revisar de forma periódica, e nos termos previstos neste Manual, as normas e os regulamentos internos da Maud, a fim de garantir que estejam condizentes com a lei e regulamentação aplicável, bem como que sejam sanadas eventuais dúvidas ou lacunas que possam surgir ao longo do exercício das atividades da Maud; (iii) supervisionar o cumprimento pelos Colaboradores das normas e regulamentos internos da Maud, mediante a adoção de medidas internas específicas para executar as políticas na rotina diária da Maud; (iv) examinar casos de violação ou potencial violação deste Manual por parte de um Colaborador e submetê-los ao Comitê de *Riscos e Compliance* para adoção das medidas cabíveis para sanar prontamente a violação ou potencial violação e punir o Colaborador, conforme aplicável; (v) providenciar o encaminhamento de denúncia sobre eventuais atos de fraude, improbidade, corrupção, PLDFTP e terrorismo às autoridades competentes, conforme aplicável; (vi) avaliar possíveis operações consideradas de suspeitas de lavagem de dinheiro e financiamento de terrorismo e, conforme aplicável, providenciar o seu encaminhamento para o COAF; (vii) instruir os Colaboradores a respeito das regras contidas neste Manual e das regras de compliance e PLDFTP aplicáveis às suas atividades; (viii) organizar e supervisionar o treinamento dos Colaboradores, de acordo com as regras de treinamento contidas neste Manual; (ix) garantir que as notificações a respeito do descumprimento ou potencial descumprimento deste Manual, da lei ou regulamentação aplicável sejam tratadas de modo confidencial e imparcial, exceto nos casos previstos neste Manual; (x) apoiar e incentivar atividades e programas de compliance.

2.8. O Comitê de *Riscos e Compliance* corresponde ao fórum de definição, revisão e avaliação da aderência às normas determinadas pelos órgãos de regulação e autorregulação e às normas de conduta e ética estabelecidas nas políticas internas da Maud.

2.9. As decisões tomadas pelo Comitê de *Riscos e Compliance* serão formalizadas em ata ou e-mail encaminhado aos membros e participantes, de imediato. Visando a mitigação de potenciais conflitos de interesses, não poderão votar os membros que se encontrem em posição de conflito de interesses em

relação à matéria deliberada. Especificamente, os membros do Comitê de *Riscos e Compliance* que representem alguma das áreas de Negócios não poderão votar caso a matéria em questão diga respeito diretamente a sua área de atuação, a si próprio ou a Colaboradores sob sua supervisão direta. O Comitê de *Riscos e Compliance* tem plena autonomia para executar as suas funções, detalhadas neste Manual. Sempre que julgar necessário, o Comitê de *Riscos e Compliance* poderá solicitar o apoio de consultores externos para a análise de suas questões. Este Comitê se reúne no mínimo trimestralmente, podendo ser convocado extraordinariamente por qualquer de seus membros, sempre que julgue necessário, sendo instalado necessariamente com a presença do Diretor de *Compliance*, ou seu substituto, representando a área de *Compliance*. Os assuntos tratados por este Comitê são estritamente confidenciais.

2.10. São atribuições do Comitê de *Riscos e Compliance*, sem prejuízo de outras atribuições descritas nas outras políticas internas da Maud: (i) implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles; (ii) propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores; (iii) definir, divulgar e revisar os procedimentos deste Manual, do Código de Ética e Conduta e demais políticas internas da Maud, bem como as estratégias para o desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências; (iv) apurar todas as denúncias e casos trazidos ao Comitê acerca do não cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual ou no Código de Ética e Conduta, assim como avaliar as demais situações que não foram previstas nas políticas internas, inclusive avaliando a necessidade de comunicação aos órgãos reguladores; (v) fornecer orientação aos Colaboradores em casos de dúvidas quanto à aplicação das políticas internas que não puderem ser esclarecidas isoladamente pelo Diretor de *Compliance*; (vi) designar um substituto do Diretor de *Compliance*, ou um responsável temporário para cumprir suas funções, em caso de ausência; (vii) definir e aplicar eventuais sanções aos Colaboradores.

III. ABRANGÊNCIA

3.1. Este Manual se aplica a todos os todos os sócios, administradores, empregados, funcionários permanentes ou temporários, estagiários, fornecedores, parceiros e prestadores de serviços da Maud ("Colaboradores").

3.2. O Diretor de *Compliance* deverá entregar uma cópia deste Manual a todos os Colaboradores, e sempre que tal documento for modificado. Mediante o recebimento deste Manual, o Colaborador deverá confirmar que leu, entendeu e cumpre com todos os termos deste Manual, mediante assinatura do termo de adesão que deverá seguir o formato previsto no Anexo I.

3.3. Todas as matérias de violações a obrigações de *compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas ao Diretor de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *compliance*, e submeter o caso ao Comitê de *Riscos e Compliance* para aplicação das sanções aplicáveis.

3.4. O Colaborador estará, ainda, sujeito às penalidades cabíveis, especialmente às previstas na legislação trabalhista, civil e penal, que serão, quando a lei assim exigir, objeto de tutela judicial específica. Será garantido ao Colaborador em questão amplo direito de defesa.

3.5. Conforme previsto no Código de Ética e Conduta, as penalidades devem sempre ser proporcionais às ações cometidas, sendo vedada qualquer aplicação arbitrária por parte do Comitê de *Riscos e Compliance*. Devem ser considerados como fatores decisórios para a aplicação da penalidade: a conduta habitual do Colaborador, a procedência do reporte, os fatos averiguados, hipóteses de reincidência, entre outros.

3.6. Conforme previsto no Código de Ética e Conduta, poderão ser aplicadas, entre outras, (i) penas de advertência, (ii) suspensão, (iii) desligamento ou (iv) demissão por justa causa, sem prejuízo do direito da Maud de pleitear indenização pelos eventuais prejuízos suportados.

3.7. É dever de todos os Colaboradores, sempre que tiverem conhecimento de uma violação ou atos que contrariem os princípios deste Manual, bem como das políticas institucionais, da má conduta, ou ainda, se suspeitarem ou souberem de fatos que possam prejudicar a Maud, reportar a violação ou a suspeita ao superior imediato e à área de *Compliance*, ou fazer uma denúncia anônima nos termos do Código de Ética e Conduta.

IV. PROCEDIMENTOS

4.1 Revisão periódica e preparação de relatório

4.1.1. O Diretor de *Compliance* deverá revisar anualmente este Manual para verificar a adequação das políticas e procedimentos aqui previstos e sua efetividade, submetendo para revisão final ao Comitê de *Riscos e Compliance*.

4.1.2. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as incorreções do período anterior, e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pela Maud.

4.1.3. Nos termos do art. 25 da Resolução CVM 21, o Diretor de *Compliance* deve encaminhar aos órgãos da administração, até o último mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação do Diretor de *Compliance* a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las. O relatório referido no parágrafo acima deverá ficar disponível para a CVM na sede da Maud.

4.2. Política de Treinamento

4.2.1. A Maud possui um processo de treinamento inicial e um programa de continuidade a respeito dos conhecimentos sobre as políticas internas, inclusive deste Manual, aplicável a todos os Colaboradores,

especialmente àqueles que tenham acesso a Informações Internas e/ou Informações Confidenciais (conforme definição abaixo) e/ou participem do processo de decisão de investimento.

4.2.2. O Diretor de *Compliance* deverá conduzir sessões de treinamento com os Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste Manual. A cada processo, os Colaboradores assinarão termo comprovando a participação no respectivo treinamento.

4.2.3. O Diretor de *Compliance* poderá ainda promover treinamentos extraordinários sempre que houver alteração nas normas que regulam as atividades da Maud, ou ainda, visando tratar de casos concretos ocorridos dentro ou fora da instituição.

4.2.4. Os materiais, carga horária e grade horária serão definidos pelo Diretor de *Compliance*, que poderá, inclusive, contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

V. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO

5.1. Nos termos do Artigo 27, III e Artigo 28, II, da Resolução CVM 21, a Maud adota procedimentos e regras de condutas para preservar Informações Internas e Informações Confidenciais (definição abaixo) e permitir a identificação das pessoas que tenham acesso a elas.

5.2. Para fins deste Manual, consideram-se "Informação(ões) Interna(s)": aquelas que dizem respeito sobre os negócios ou operações da Maud que, embora não necessariamente confidenciais, garantem algum certo grau de privacidade. Exemplos incluem, mas não se limitam, a determinadas informações sobre os controles internos ou procedimentos operacionais da Maud, e informações sobre vendedores, fornecedores, contratados e investimentos ou qualquer informação cuja divulgação possa ser exigida por lei ou por autoridade competente.

5.2.1. Para fins deste Manual, consideram-se "Informação(ões) Confidencial(is)": aquelas consideradas privadas, particulares ou confidenciais ou recebidas pelos Colaboradores, a respeito de atividades ou negócios de clientes, incluindo dados pessoais e dados pessoais sensíveis, nos termos da 13.709, de 14 de agosto de 2018, conforme alterada ("LGPD"). Informações Confidenciais podem estar em formato físico (escritas em papel, em e-mail ou gravadas em disco) ou não. Informações Confidenciais incluem informações da Maud ou de seus clientes, que incluem, dentre outras: sigilos comerciais, inovações, planos de marketing, planos empresariais, relações com investidores e informações sobre investidores no geral, além de termos de quaisquer contratos, dados financeiros, modelos financeiros, pesquisa e desenvolvimento, previsões, processos, comunicações internas, consultoria jurídica, códigos de acesso a computadores, posições de investimento, intenções e estratégias comerciais, estratégias de investimento, configurações de sistemas de computadores e outras informações de sistemas e dados de desempenho, cujas informações derivam valor econômico independente, efetivo ou potencial, por não serem conhecidas.

5.2.2. Para fins deste Manual, consideram-se "Informação(ões) Pública(s)": aquelas que a Maud e seus Colaboradores podem disponibilizar ao público em geral. Inclui, por exemplo, informações disponíveis no

website da Maud acessíveis ao público, conteúdo acessível ao público em páginas de mídias sociais ou perfis gerenciados pela Maud e informações acessíveis pelo público em geral nos arquivamentos regulamentares da Maud.

5.2.3. Para fins deste Manual, consideram-se "Informação(ões) Privilegiada(s)": qualquer Informação Confidencial e/ou Informação Interna que possa influir de modo ponderável: (a) na rentabilidade dos valores mobiliários administrados pela Maud; (b) na decisão de comprar, vender ou manter cotas de fundos de investimento administrados pela Maud; e (c) na decisão de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Maud.

5.3. Os Colaboradores não devem utilizar as Informações Confidenciais e/ou Informações Internas em seu próprio benefício ou em benefício de qualquer outra parte que não a Maud. Além disso, os Colaboradores não podem divulgar as Informações Confidenciais e Informações Internas a pessoas fora da Maud, exceto no cumprimento dos negócios da Maud e de maneira consistente com os interesses da Maud, após consideração das garantias de procedimento apropriadas e de qualquer outra política de privacidade aplicável, ou conforme exigido pela regulamentação aplicável após consulta ao Diretor de Compliance. Os Colaboradores estão proibidos a compartilhar cópias físicas ou eletrônicas de arquivos que contenham Informações Confidenciais, bem como a postar ou discutir as Informações Confidenciais em redes sociais ou em sites de relacionamento profissional, blogs e salas de bate papo, sendo que a divulgação deverá sempre anteceder a anuência prévia do Diretor de Compliance.

5.4. O acesso às Informações Confidenciais e Informações Internas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Maud.

5.5. De modo a proteger as Informações Confidenciais e Informações Internas, os Colaboradores se comprometem a:

a) não retirar ou transmitir qualquer Informação Confidencial e/ou Informação Interna das instalações da Maud, salvo na hipótese de trabalho remoto (home office) devidamente autorizado pelo Diretor de *Compliance*, ou se for absolutamente necessário, e desde que autorizado pelo Diretor de *Compliance*, devendo o Colaborador sempre possuir a autorização para dispor da referida Informação Confidencial e/ou Informação Interna conforme suas atribuições profissionais. Em qualquer hipótese, os Colaboradores somente podem utilizar recursos computacionais e dispositivos móveis disponibilizados pela Maud, os quais possuem os mecanismos de proteção necessários;

b) agir com cautela na exibição de documentos ou discutir as informações com cautela em locais públicos como elevadores, restaurantes, aviões ou na presença de pessoas que não sejam Colaboradores;

c) agir com cautela em relação aos documentos que contêm Informação Confidencial e/ou Informação Interna quando utilizá-los em salas de conferência ou no descarte de documentos, em mesas, lixos, banheiros, ou em qualquer outro local onde a informação possa ser vista ou mantida;

d) utilizar métodos aprovados pela área de Tecnologia da Informação (TI) da Maud para copiar ou transmitir dados, com relação, em particular, a grandes volumes de informação;

e) abrir com cautela comunicações eletrônicas e anexos para evitar a entrada de *spyware* e *malware;*
f) revisar e-mails antes do envio, para confirmar que os destinatários estão adequados e os anexos estão selecionados de forma correta;
g) nunca divulgar senhas de computador ou correio de voz, ou códigos de acesso a sites para uma pessoa não autorizada; e
h) compartilhar com cautela as Informações Confidenciais e Informação Interna com qualquer pessoa na Maud.

5.6. A Maud restringe e controla o acesso de pessoas às dependências da sua sede e aos documentos e informações de sua propriedade, armazenados física ou virtualmente, por meio de login e senhas de segurança apropriada individuais para cada Colaborador. O Colaborador deve manter em local seguro suas senhas e não divulgar a terceiros em nenhuma hipótese.

5.7. O acesso eletrônico a Informações Confidenciais e a Informações Internas é controlado a partir do usuário atribuído a cada Colaborador de acordo com suas atribuições profissionais. No momento do cadastro, o Diretor de Compliance é consultado para atribuir o nível de prerrogativas de acesso eletrônico pelo respectivo Colaborador, o que pode ser revisado se necessário. O acesso é imediatamente cancelado em caso de desligamento do Colaborador.

5.8. A Maud implementa, ainda, duplo nível de autenticidade para acesso aos seus sistemas e arquivos, por meio da ferramenta Office 365 e do acesso Virtual Private Network (VPN).

5.9. As restrições da Maud sobre a divulgação e uso de Informações Confidenciais e Informações Internas continuarão em vigor após o término ou modificação de um vínculo empregatício de um Colaborador com a Maud, a menos que uma permissão por escrito específica seja obtida do Diretor de Gestão ou do Diretor de Compliance.

5.10. Sob supervisão do Diretor de Compliance, a área de TI conduzirá testes semestrais para garantir o devido cumprimento destas normas.

5.11. As Informações Privilegiadas precisam ser mantidas em sigilo por todos que as acessarem, seja em função da prática da atividade profissional ou de relacionamento pessoal. Em caso de o Colaborador ter acesso a uma Informação Privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de Compliance, não podendo transmiti-la a outras pessoas, inclusive membros da Maud, profissionais do mercado, amigos, parentes, tampouco utilizá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se relatar a dúvida ao Diretor de Compliance.

5.12. A prática de qualquer ato em violação das disposições acima pode sujeitar o infrator à responsabilidade civil e criminal, por força do artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976, bem como à imposição de penalidades nesse âmbito, conforme a Resolução CVM nº 44, de 23 de agosto de 2021, conforme atualizada.

VI. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

6.1. É de responsabilidade de todos os Colaboradores, prestadores de serviço da Maud e prestadores de sistemas da Maud a proteção da segurança e integridade das informações e equipamentos de informática da Maud, em observância desta política.

6.2. As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos envolvidos. As consequências para as atividades da Maud podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

6.3. Além de mal funcionalidade dos seus sistemas e aparelhos eletrônicos, a Maud pode ainda estar sujeita a ataques cibernéticos. Os métodos mais comuns de ataques cibernéticos, segundo as melhores práticas sobre o tema, são os seguintes: (i) *Malware*: softwares desenvolvidos para corromper computadores e redes; (ii) Vírus: software que causa danos a máquina, rede, softwares e banco de dados; (iii) Cavalo de Troia: mecanismo que aparece dentro de outro software e cria uma porta para a invasão do computador; (iv) *Spyware*: software para coletar e monitorar o uso de informações; (v) *Ransomware*: software que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido; (vi) Engenharia Social: método de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito; (vii) *Pharming*: mecanismo de direcionamento do usuário para site fraudulento, sem o seu conhecimento; (viii) *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; (ix) *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; (x) *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; (xi) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque; (xi) Ataques de DdoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de inúmeros computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; (xii) Invasões (*advanced 9ersistente threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

6.4. A Maud possui diversos procedimentos de prevenção e proteção de dados, dentre eles: (i) todos os recursos computacionais e dispositivos móveis utilizados pelos Colaboradores são de propriedade da Maud ou homologados por sua área de TI; (ii) todos os sistemas utilizados pelos Colaboradores foram adquiridos pela Maud; (iii) não é permitida a utilização de notebooks, tablets ou outros hardwares adquiridos pelos Colaboradores para exercer as atividades da Maud, salvo expressa permissão do Diretor de *Compliance*, após homologação e registro do aparelho pela área de TI; (iv) todos os computadores utilizados por Colaboradores têm por objetivo o desempenho das atividades profissionais na Maud; (v) para contratação do sistema de nuvem, serão exigidos os melhores padrões de cibersegurança, solicitando-se documentos que atestem os procedimentos de cibersegurança e que comprovem a capacidade técnica no prestador de

serviços, de modo que a contratação deve ser aprovada pela área de TI em conjunto com o Diretor de Compliance; (vi) todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de TI, mediante supervisão e aprovação do Diretor de Compliance; (vii) é desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada pelo TI e Diretor de Compliance; (viii) é desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores; (ix) monitoramento contínuo e sem periodicidade dos controles existentes neste Manual, realizado pela área de TI sob supervisão do Diretor de Compliance; (x) monitoramento contínuo e sem periodicidade dos controles existentes nesse Manual, realizado pela área de TI sob supervisão do Diretor de Compliance.

6.5. São procedimentos para disponibilização e uso dos computadores: (i) a cada novo Colaborador, o Diretor de *Compliance* deve autorizar, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos; (ii) todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área de TI, mediante supervisão e aprovação do Diretor de Compliance; (iii) o Diretor de Compliance autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário; (iv) cada computador tem o seu usuário gestor, que é responsável por esse equipamento, sendo o controle das máquinas de responsabilidade da área de TI, mediante supervisão e aprovação do Diretor de Compliance; (v) a identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Maud é sua assinatura eletrônica no servidor da Maud; (vi) o Colaborador não deve compartilhar nem compartilhar a sua senha com terceiros e outros Colaboradores; (vii) é permitida apenas número limitado de tentativas de autenticação de senha, sendo que a incorreção bloqueará o acesso do Colaborador, o qual apenas poderá ser reestabelecido através de solicitação à área de TI; (viii) todos os eventos de login e alteração de senhas são auditáveis e rastreáveis,

6.6. Conforme as melhores práticas de mercado, a Maud desenvolveu plano de resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais e/ou Informações Internas ou outra falha de segurança. O plano de resposta consiste em:

(a) a área de TI, sob supervisão do Diretor de Compliance, deve, conforme aplicável, entre outros, (i) verificar e auditar os logs; (ii) criar laudo pericial contendo as informações que foram potencialmente vazadas; (iii) executar aplicativos para eliminar aplicativos indesejados; (iv) desinstalar software; (v) executar varreduras off-line para descobrir quaisquer ameaças adicionais; (vi) formatar e reconstruir o sistema operacional; (vii) substituir os dispositivos de armazenamento; (viii) reconstruir sistemas de redes; (ix) restaurar dados provenientes do backup realizado diariamente;

(b) o Diretor de Compliance deve, conforme aplicável, (i) criar relatório baseado no laudo pericial elaborado pela área de TI, constatando eventuais danos e sugerindo eventuais soluções, bem como classificar o nível de severidade do evento; (ii) elaborar notificação a clientes afetados informando o vazamento de informações, caso aplicável, bem como a Autoridade Nacional de Proteção de Dados (ANPD);

(c) o Diretor de Compliance deve, conforme aplicável, analisar dados eventualmente perdidos e seu impacto no planejamento contábil e valor dos ativos;

(d) se necessário, poderá ser contratada empresa especializada para o combate do evento identificado e/ou respostas a eventual dano; e

(e) arquivamento dos materiais e documentos relacionados ao evento e às medidas adotadas

6.7. Os controles internos devem ser efetivos e contínuos, e revistos e atualizados de forma periódica, a fim de identificar e tratar tempestivamente as fragilidades.

6.8. O monitoramento dos controles existentes e estabelecidos nesta política serão realizados e executados pela área de TI, sob supervisão do Diretor de Compliance. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

6.9. Quanto às práticas de atenção às contingências, continuidade de negócios e recuperação de desastres, a Maud também possui Plano de Continuidade de Negócios – PCN com o objetivo de fortalecer a resiliência da organização e a sustentabilidade de seus produtos e serviços essenciais para o negócio, mesmo em situações adversas de crises e desastres. Ela estabelece as diretrizes e os princípios básicos necessários para uma resposta emergencial adequada ao evento, e à recuperação e restauração dos níveis de normalidade operacional.

6.10. O Plano de Continuidade de Negócios assegura à Maud e seus Colaboradores a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos. Os possíveis cenários de indisponibilidade são:

a) Perda total do acesso às dependências da sede da Maud e/ou dos recursos abrigados nela;
b) Perda total ou parcial da estrutura tecnológica (serviços e/ou comunicação);
c) Perdas temporárias ou permanentes de recursos.

6.11. Para contingência/desastre que provoquem efeitos menores, o Plano de Continuidade de Negócios poderá ser parcialmente aplicado, conforme entendimento das equipes envolvidas no processo de ativação do plano, horário de ocorrência, processos e atividades pendentes, tempo de recuperação comparado ao tempo de ativação completa e quantidade de recursos indisponíveis.

6.12. O Plano de Continuidade de Negócios não inclui procedimentos de recuperação para serviços terceirizados essenciais à continuidade dos negócios da Maud. Para estes casos, os contratos devem possuir acordos de níveis de serviço, os quais endereçam a responsabilidade da contraparte pela respectiva retomada operacional, em cenários de contingência/desastre, de forma a atender as necessidades de negócios da Maud.

VII. POLÍTICA DE PLDFTP

7.1. Para fins deste Manual, "PLDFTP" significa prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.

7.2. O termo "lavagem de dinheiro" abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal para simular uma origem legítima. Já o "financiamento ao terrorismo" tem como fundamento a existência de indícios ou provas da prática de terrorismo, de seu financiamento ou de atos a ele correlacionados, por pessoas naturais, jurídicas ou entidades. O art. 2º da Lei nº 13.260/2016, conforme alterada, define como terrorismo a prática de determinados atos pré-identificados por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública. A Maud e seus Colaboradores estão comprometidos com a atividade de PLDFTP com relação a seus negócios, com o objetivo de detectar e deter a ocorrência de lavagem de dinheiro, financiamento ao terrorismo e outras atividades ilegais.

7.3. A prática de atos de financiamento ao terrorismo e proliferação de armas de destruição em massa prescinde de identificação de montante relevante ou substancial para auxílio ou financiamento de tais práticas, bastando a identificação de qualquer volume financeiro utilizado para tal fim para que sejam tomadas as medidas de reporte e combate aqui previstas.

7.4. A Maud e seus Colaboradores devem cumprir a totalidade de regras que previnem a lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, inclusive, sem limitação, a Lei nº 9.613, de 3 de março de 1998, conforme alterada; a Lei nº 13.260, de 16 de março de 2016, conforme alterada; e a Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM 50"). O envolvimento em atividade de lavagem de dinheiro, ainda que de forma inadvertida, pode resultar em penalidades civis e criminais para a Maud, seus clientes e/ou seus Colaboradores, bem como danos reputacionais.

7.5. O Diretor de *Compliance*, nos termos do art. 8º da Resolução CVM 50, é responsável por essa política, bem como por todos os preceitos concernentes à PLDFT, devendo realizar treinamento com os Colaboradores, para reconhecer e combater a lavagem de dinheiro e o financiamento ao terrorismo e proliferação de armas de destruição em massa, conforme as disposições do item 4.2. deste Manual. O Diretor de *Compliance* deve providenciar novos treinamentos no caso de mudança da legislação e regulamentação aplicáveis.

7.6. Proteger a Maud de ser inadvertidamente contaminada por pessoas que praticam lavagem de dinheiro é responsabilidade de cada Colaborador. Nenhum Colaborador deve participar ou facilitar qualquer atividade de lavagem de dinheiro. O descumprimento desta política sujeita os Colaboradores faltosos à ação disciplinar, inclusive (sem limitação) a rescisão do contrato de trabalho, bem como possíveis penalidades civis e criminais.

7.7. A Maud adota postura rígida na contratação de seus Colaboradores. Antes do ingresso na empresa os candidatos devem ser entrevistados pelos administradores da Maud. Requisitos ligados à reputação no mercado e perfil serão avaliados, bem como os antecedentes profissionais do candidato.

7.8. A Maud adota metodologia de avaliação de riscos que classifica a sua exposição à lavagem de dinheiro e financiamento ao terrorismo e proliferação de armas de destruição em massa em determinadas operações que costumam ser por ela realizadas. Os parâmetros gerais da metodologia de riscos estão elencados no Anexo II ao presente Manual e são amparados, sobretudo, na análise da contraparte das ordens e na precificação do ativo transacionado.

7.9. Qualquer Colaborador que suspeite da possibilidade de ocorrência de atividades de lavagem de dinheiro envolvendo a Maud ou seus clientes deverá alertar o Diretor de *Compliance*, comunicando todos os detalhes possíveis. Nesse caso, o Diretor de *Compliance* deverá instituir investigações para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão, conforme a legislação e regulamentação aplicável. O Diretor de *Compliance* deve, ainda, realizar comunicação ao Conselho de Controle de Atividades Financeiras ("COAF"), respeitando-se o prazo de 24 (vinte e quatro) horas, contadas a partir da conclusão da análise que caracterizou a atipicidade da operação.

7.10. Caso não tenha sido identificada nenhuma atividade suspeita, o Diretor de Compliance deverá encaminhar à CVM comunicação de não ocorrência de transações ou propostas de transações passíveis de serem comunicadas, até o último dia útil de abril de cada ano, por meio de mecanismos estabelecidos no convênio celebrado entre a CVM e o COAF.

7.11. O Diretor de Compliance deve encaminhar anualmente, até o último dia útil de abril de cada ano, o relatório anual de avaliação interna de risco de PLDFTP, nos termos do art. 6º da Resolução CVM 50.

7.12. O referido relatório deverá contemplar, além da avaliação interna de risco, nos termos do art. 5º da Resolução CVM 50: (a) a identificação e análise das situações de risco de PLDFTP, considerando as respectivas ameaças, vulnerabilidades e consequências; (b) número de operações analisadas e situações atípicas detectadas, além do número de comunicações de operações suspeitas e eventual declaração negativa; (c) a apresentação dos indicadores de efetividade, incluindo a tempestividade acerca das atividades de detecção, análise e comunicação de operações ou situações atípicas; (d) a apresentação, se for o caso, de recomendações visando mitigar os riscos identificados do exercício anterior que ainda não foram devidamente tratados; e (e) a indicação da efetividade das recomendações adotadas em relação ao relatório respectivamente anterior.

7.13. Os Colaboradores, sujeitos à supervisão do Diretor de Compliance, devem manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente na hipótese de existência de investigação comunicada formalmente pela CVM. Cada fundo de investimento deve conter registros próprios, segregados dos demais existentes sob a gestão da Maud.

7.14. O Diretor de Compliance deve adotar procedimentos para assegurar que a Maud previna danificação, falsificação, destruição ou alteração indevida dos livros e registros.

VIII. POLÍTICA DE KNOW YOUR CLIENT (KYC)

8.1. A Maud não pretende praticar atividade de distribuição e não possui atualmente as autorizações legais e regulatórias necessárias para tanto.

8.2. A Maud presta serviços de administração carteira e estrutura soluções financeiras através da constituição de fundos de investimento. Possui contato direito com seus clientes e, para efeitos de KYC, requer informações cadastrais e de *suitability* conforme regulamentação aplicável e realiza auditoria independente para efeitos de PLDFTP. Neste último caso, no *onboarding*, a Maud utiliza-se do sistema AML Due Diligence e Pantherae da empresa Ethquo que compila todas as informações públicas disponíveis, incluindo informações judiciais, de crédito e imprensa, e para monitoramento de cada um de seu clientes, utiliza-se da E-guardian da empresa Advise.

8.3. Sem prejuízo, no limite de suas atribuições como gestora dos fundos, quando alocando recursos de seus clientes em fundos administrados e geridos por terceiros, a Maud questionará periodicamente os administradores fiduciários dos fundos sobre os testes que realizam na base de investidores dos fundos de investimento sob sua gestão, bem como qual a governança adotada pelos administradores fiduciários para prevenção à lavagem de dinheiro e financiamento ao terrorismo, fiscalização de prestadores de serviços quanto a essa temática, sobretudo aos eventuais distribuidores contratados.

8.4. Caso a Maud passe a realizar a distribuição dos seus fundos e estabelecer relacionamento com os cotistas dos seus fundos, obtendo as autorizações legais e regulatórias necessárias para tanto, este Manual deverá ser imediatamente atualizado para prever regras específicas e detalhadas de KYC.

IX. POLÍTICA DE COMBATE À CORRUPÇÃO

9.1. Segundo dispõe a Lei nº 12.846, de 1º de agosto de 2013, conforme atualizada ("Lei Anticorrupção"), constituem atos lesivos à administração pública, nacional ou estrangeira, todos aqueles praticados pelas pessoas jurídicas que atentem contra o patrimônio público nacional ou estrangeiro; contra princípios da administração pública; ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos: (a) prometer, oferecer ou dar, direta ou indiretamente, vantagem imprópria a agente público, ou a terceira pessoa a ele relacionada; (b) financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos que violam a Lei Anticorrupção; (c) utilizar-se de modo impróprio de terceiro, seja pessoa física ou jurídica, para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados em violação de qualquer lei; (d) no tocante a licitações e contratos: (i) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público; (ii) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público; (iii) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; (iv) fraudar licitação pública ou contrato dela decorrente; (v) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; (vi) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato

convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou (vii) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública; e (e) dificultar atividades de investigação ou fiscalização por órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

9.2. Considera-se "administração pública estrangeira", para os fins desta política, os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro. Equiparam-se à administração pública estrangeira as organizações públicas internacionais.

9.3. Considera-se agente público estrangeiro, para os fins desta política, quem, ainda que transitoriamente ou sem remuneração, exerça cargo, emprego ou função pública em órgãos, entidades estatais ou em representações diplomáticas de país estrangeiro, assim como em pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro ou em organizações públicas internacionais.

9.4. Nenhum Colaborador deve participar ou facilitar qualquer atividade de corrupção. O descumprimento desta política sujeita os Colaboradores faltosos à ação disciplinar, inclusive a rescisão do contrato de trabalho, bem como possíveis penalidades civis e criminais. Os Colaboradores estão obrigados a denunciar de imediato ao Diretor de Compliance qualquer atividade suspeita que se enquadre na descrição acima.

9.5. A Maud utiliza seus melhores esforços para monitorar todos os Colaboradores da instituição, de forma a garantir que estes atuem em observância a Lei de Anticorrupção e sua regulamentação, respeitando e praticando, na medida de suas atividades e possibilidades, os atos referentes ao Programa de Integridade disposto no Decreto n.º 11.129, de 11 de julho de 2022.

9.6. No tocante às relações com agentes públicos, os Colaboradores devem agir de modo a prevenir e, se for o caso, remediar situações de conflito de interesses, que podem ocorrer tanto em relação à Maud e seus Colaboradores, quanto em relação à Maud e o poder público. Nesse sentido, em linha com as práticas vedadas descritas acima e conforme Lei Anticorrupção, os Colaboradores estão proibidos de oferecer, prometer, fazer, autorizar ou proporcionar, diretamente ou através de intermediários, qualquer vantagem indevida a agentes públicos, com a intenção de influenciar ou retribuir qualquer ação oficial ou decisão do referido agente, em favor do próprio Colaborador e/ou da Maud, bem como consentir com o recebimento, em nome próprio ou em nome da Maud, de qualquer tipo de vantagem que possa ser interpretada como forma de pagamento decorrente de atos lesivos à administração pública, principalmente os relacionados à prática de corrupção.

9.7. Com o objetivo de garantir a eficácia e a aplicação das vedações acima, quaisquer contatos com agentes públicos, seja através de correspondência eletrônica, conferências telefônicas, reuniões presenciais, ou reuniões virtuais poderão ser supervisionados pelo Diretor de Compliance.

X. POLÍTICA DE SELEÇÃO, CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS PRESTADORES DE SERVIÇOS

10.1. Previamente à contratação de terceiros prestadores de serviço em nome da Maud, o Colaborador que desejar contratar o terceiro deve fornecer ao Diretor de *Compliance* informações necessárias para realização de diligência prévia do terceiro, com objetivo de verificar (i) sua adequação aos requisitos legais e regulatório; (ii) eventuais conflitos de interesses; (iii) a sua capacidade de prestar os serviços a serem contratados; e (iv) o custo da prestação de serviço, sempre visando ao melhor interesse da Maud.

10.2. Nesse sentido, serão solicitados para todas as atividades não sujeitas à supervisão e regulamentação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA): (i) qualificação completa da sociedade; (ii) comprovação de poderes de representação; (iii) listagem do nome e qualificação dos sócios e administradores; (iv) data de início das atividades; (v) pesquisa de mercado a respeito da qualidade do serviço prestado pelo terceiro, experiência no serviço contratado, reputação, custo do serviço em comparação com outros prestadores do mesmo serviço; (vi) confirmação de ausência de conflitos de interesse, ainda que em potencial, com o terceiro e, se necessário; e (vii) visita ao escritório do terceiro a ser contratado e/ou conversas com os principais executivos. Para as atividades sujeitas à supervisão e regulamentação da ANBIMA, além dos requisitos anteriores, será solicitado o preenchimento do respectivo Questionário ANBIMA de Due Diligence. A MAUD aplica referido questionário para contratação de (i) custodiante, (ii) escriturador, (iii) controlador do ativo, (iv) controlador do passivo e (v) corretoras de títulos e valores mobiliários. O questionário deve ser respondido por profissional(is) com poderes de representação. Qualquer alteração em relação às respostas enviadas e aos documentos encaminhados após o preenchimento destes questionários devem ser enviadas à instituição que contratou a prestação de serviço em até cinco dias úteis da referida alteração.

10.3. Os terceiros aprovados para contratação e efetivamente contratados pela Maud devem ser monitorados por meio de avaliações periódicas, nas quais serão verificados novamente os critérios acima definidos para cada tipo de terceiro, bem como a qualidade do serviço que vem sendo prestado. O monitoramento é de responsabilidade do Diretor de *Compliance*, por meio de diligências de revisão/atualização da documentação coletada para fins da contratação inicial.

10.4. A contratação de terceiros é necessariamente formalizada por meio de contrato escrito, observados os requisitos legais e regulamentares aplicáveis. A contratação de terceiros em nome dos fundos geridos pela Maud é necessariamente formalizada por meio de contrato escrito, observados os requisitos legais e regulamentares aplicáveis, especialmente o conteúdo mínimo previsto no art. 19 do Código ANBIMA de Administração de Recursos de Terceiros. O início das atividades do terceiro deve ser vinculado à formalização da contratação e não devem ser realizados pagamentos ao terceiro antes da celebração do contrato. O Colaborador deve requerer, ainda, que o terceiro preencha e consinta com Declaração contida no Anexo III deste Manual, indicando que não participa de práticas de corrupção, lavagem de dinheiro e financiamento ao terrorismo.

10.5. Todos os documentos relacionados à contratação de terceiros serão arquivados ou armazenados digitalmente pela Maud pelo prazo mínimo de 5 (cinco) anos.

XI. POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES

11.1. A Maud não desempenha atividades alheias à administração de recursos de terceiros, na qualidade de "gestor de recursos", tampouco realiza a distribuição de cotas de fundos de investimento sob sua gestão; de todo modo, minimiza conflitos de interesses e garante a segregação institucional e hierárquico funcional das suas atividades adotando ao menos as seguintes medidas: (a) implementação de controles de acesso às pastas e diretórios virtuais de acordo com a área e função de cada Colaborador e restrição de acesso a determinadas informações; (b) discussão de matérias capazes de gerar conflito de interesse somente em ambientes reservados; (c) não submissão do Diretor de Compliance à área de gestão de recursos; (d) proibição de cumulação de função para Colaboradores responsáveis pela área de gestão de recursos com qualquer área que possa causar conflito de interesses; (e) regras para preservação e manutenção de sigilo às Informações Confidenciais e/ou restrição de divulgação de Informações Internas; (f) implementação e manutenção de programa de treinamento aos Colaboradores; (g) implementação de controles que permitam identificar as pessoas que tenham acesso aos arquivos e às Informações Confidenciais e às Informações Internas; (h) informação aos investidores a respeito de outras sociedades que passem a compor o grupo econômico da Maud; (i) manutenção de testes periódicos de segurança para os sistemas de informação, em especial para aqueles mantidos em meio eletrônico; e (j) estabelecimento de Política de Investimento Pessoais para os Colaboradores.

11.2. A Maud adota, ainda, segregação física das suas atividades perante terceiros. O atendimento a terceiros, quando aplicável, nas dependências da Maud ocorrerá nas salas de visitas e reuniões.

11.3. Caso a Maud venha a compartilhar suas instalações com outras instituições, as seguintes medidas deverão ser adotadas: (i) segregação física; (ii) segregação funcional; (iii) segregação informacional; (iv) segregação tecnológica e sistêmica.

XII. POLÍTICA DE SELEÇÃO E ALOCAÇÃO DE ATIVOS

12.1. A Maud realiza a seleção e alocação dos ativos dos fundos geridos em observância da política de investimentos previstas nos respectivos regulamentos e observando a disponibilidade dos recursos em caixa dos fundos. A Maud poderá ser responsável pela gestão da carteira de múltiplos fundos.

12.2. A equipe de gestão e análise de investimento, supervisionada e auxiliada pelo Diretor de Gestão de Recursos, adota os seguintes procedimentos para seleção e alocação de ativos para os Fundos:

(a) Pesquisa: Nesta etapa, a equipe de gestão conduz uma pesquisa abrangente do mercado. Apesar de ter mais relevância no mercado nacional, a análise também se estende ao mercado internacional. A gestão possui um extenso fluxo de ofertas primárias que passam por análises, além de ativos já no mercado que apresentam pontos de compra vistos como benéficos.

(b) Aprovação do Diretor de Gestão de Recursos: Antes de prosseguir com qualquer alocação de ativos, a equipe de gestão discuti internamente e submete suas recomendações ao Comitê de Investimento, composto por três membros que podem vetar a operação. Além disso, as estruturas complexas são submetidas ao Comitê de *Riscos* e *Compliance* – que também deve aprovar a operação antes da execução da mesma. Essas etapas garantem que todas as decisões estejam alinhadas com a estratégia de investimento e buscam mitigar os riscos.

(c) Implementação: Uma vez que os ativos são aprovados, a equipe de gestão inicia o processo de implementação. Isso envolve a negociação de contratos, diligência da documentação, aprovação jurídica, a aquisição de propriedades e todas as atividades relacionadas à concretização do investimento.

(d) Acompanhamento: Após a implementação, a área de gestão monitora constantemente o desempenho de cada ativo, de acordo com parâmetros pré-estabelecidos para cada classe de investimento. O acompanhamento rigoroso ajuda a garantir que os ativos permaneçam em conformidade com as expectativas.

(e) Análise de desempenho (por fundo e consolidado): Realizamos análises detalhadas do desempenho de cada investimento individualmente e consolidamos os dados para uma visão geral da carteira. Isso nos permite avaliar o retorno sobre o investimento, medir a eficácia de nossa estratégia e fazer ajustes quando necessário. Além disso, compartilhamos regularmente relatórios de desempenho com nossos investidores para garantir total transparência.

12.3. O controle de enquadramento, riscos e liquidez, bem como o acompanhamento é realizado em conjunto com o administrador dos respectivos fundos. O mesmo procedimento deve ser utilizado em casos de investimentos em créditos privados. A Maud tem por princípio exercer a atividade de gestão de fundos de investimento com os mais elevados padrões de diligência, observados os riscos a que estão expostos os investidores, ao investirem em fundos sob sua gestão, bem como segundo as normas que regem a aplicação de recursos nessa modalidade de ativos.

12.4. Os seguintes procedimentos serão adotados anteriormente à realização dos investimentos – *pré trade*: (i) acompanhamento, pela área de gestão, das oportunidades disponíveis no mercado; (ii) definição dos limites e alçadas, considerando as características dos ativos e emissores; (iii) indicação de oportunidades de investimento, dos limites de alocação definidos nos regulamentos dos fundos; (iv) observância, em operações envolvendo empresas do conglomerado ou grupo econômico da Maud e/ou do administrador fiduciário dos fundos de investimento, os mesmos critérios utilizados em operações com terceiros, mantendo documentação de forma a comprovar a realização das operações em bases equitativas e livre de conflitos de interesse; (v) avaliar a capacidade de pagamento do devedor e/ou de suas controladas, bem como a qualidade das garantias envolvidas, caso existam; e (vi) analisar a necessidade de contratar terceiros para auxiliar na avaliação ou no acompanhamento do crédito privado, devendo realizar, para esta contratação, prévia e criteriosa análise e seleção dos contratados, conforme item X deste Manual; (vii) subsmissão dos ativos selecionados ao Comitê de Investimento.

12.5. Os seguintes procedimentos serão adotados posteriormente à realização dos investimentos – *pós trade*: (i) acompanhar o cumprimento das obrigações assumidas em cada emissão (constituição de

garantias, divulgação de informações, etc.); (ii) reportar à área de compliance os eventos extraordinários e relevantes relativos ao ativo, emissor ou setor que de alguma forma possam afetar a qualidade do crédito ou a capacidade de pagamento do emissor, bem como as respectivas ações a serem tomadas pela área de gestão; (iii) atualizar os pareceres/relatórios relativos à cada aquisição e que ainda constem nas carteiras dos fundos de investimento sob gestão, avaliando os eventos ocorridos no período; e (iv) anualmente, a área de gestão deverá realizar um relatório contendo as seguintes informações e documentos, caso existentes: relatórios de rating; relatórios de auditorias; relatórios de agentes fiduciários; certidões simplificadas da Junta Comercial de cada um dos players e, sendo o caso, alterações societárias relevantes; matrículas atualizadas dos imóveis dados em garantia e laudos de avaliação; documentação atualizada de propriedade de outros bens móveis dados em garantia e laudos de avaliação; relatórios gerados quanto a outros bens/direitos cedidos fiduciariamente em garantia.

XIII. AUDITORIA INTERNA

13.1. A auditoria interna da Maud é realizada através de empresa terceirizada, a qual possui a devida certificação para desempenho de tal atividade.

XIV. DISPONIBILIZAÇÃO

14.1. Nos termos do art. 16, inciso III, da Resolução CVM nº 21/21, o Manual estará disponível na página da Maud na rede mundial de computadores.

XV. APROVAÇÃO DESTE MANUAL

15.1. Este Manual foi devidamente aprovada pelo Comitê de *Riscos* e *Compliance*.

HISTÓRICO DAS ATUALIZAÇÕES			
DATA	**VERSÃO**	**AUTOR**	**REVISOR**
Janeiro de 2024	1.0	Victor Hideki Obara	Marcello Vidigal

ANEXO I – Termo de Adesão

Eu, ……., inscrito no CPF sob o nº ……., declaro para os devidos fins, que:

1. Estou ciente da existência do "Manual de Controles Internos" ("Manual") da Maud Capital Gestora de Ativos Ltda.
2. Compreendi o inteiro teor do Manual, com o qual declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme as obrigações definidas no Manual).
3. Tenho ciência e comprometo-me a observar integralmente os termos do Manual sob pena da aplicação das sanções cabíveis.
4. Estou ciente e de acordo com a Política de Confidencialidade da empresa, descrita no capítulo V do Manual, e entendo que a revelação não autorizada de qualquer Informação Confidencial e/ou Informações Internas pode acarretar prejuízos irreparáveis, e que no caso de descumprimento do dever de confidencialidade nos termos deste Manual estarei sujeito à aplicação das sanções cabíveis.
5. Participei do processo de integração e treinamento inicial da Maud, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e comprometo-me a observar o Manual no desempenho das minhas atividades, bem como a participar assiduamente dos programas de treinamento da Maud.
6. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da Maud, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.
7. Assino eletronicamente o presente Termo de Adesão, pela plataforma _____, a qual reconheço como válida para fins do disposto no artigo 10, parágrafo 2° da Medida Provisória n° 2.200-2, de 2001, sendo certo que (i) ainda que assinado eletronicamente em local diverso, o local de celebração é, para todos os fins, o local abaixo indicado; e (ii) será considerada a data de assinatura deste Termo, para todos os fins e efeitos, a data indicada abaixo, não obstante a data em que a última das assinaturas eletrônicas for realizada.

[Local e data]

_____

ANEXO II - Metodologia de Avaliação de Risco e Monitoramento de PLDFTP

Com o propósito de atender ao disposto na Resolução CVM 50 e nas demais normas atinentes à PLDFTP, a Maud classificará o risco de lavagem de dinheiro e financiamento ao terrorismo e da proliferação de armas de destruição em massa das suas operações conforme metodologia de avaliação de risco elencada no presente anexo.

A referida metodologia se concentra na atividade exclusiva de gestão de recursos de carteiras de fundos de investimento sob gestão da Maud, considerando a sua não atuação na qualidade de distribuidora dos referidos veículos sob gestão, e tem por base a experiência da Maud, bem como as instruções, pareceres e orientações emanados pelos reguladores e autorreguladores brasileiros, levando em conta para as classificações ora dispostas os limites de suas atribuições enquanto gestora de recursos, ao mesmo tempo que preza pela eficiência em identificar, analisar, compreender e mitigar os riscos de PLDFTP.

São levados em conta **(a) o ambiente de negociação; (b) a formação do preço do ativo negociado; e (c) a contraparte da operação, pelo que são identificados todos os produtos e serviços ofertados pela Maud, além dos mandatos de investimento concedidos pelos fundos de investimento sob sua gestão, para classificar as operações em (i) Baixo Risco; (ii) Médio Risco; ou (iii) Alto Risco.**

Metodologia e Avaliação

Baixo Risco.

As operações classificadas com potencial de Baixo Risco são:
a) ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM.
b) ofertas públicas com esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM.
c) Ativos emitidos ou negociados por instituição financeira ou equiparada.
d) Ativos emitidos por emissores de valores mobiliários registrados na CVM.
e) Ativos de mesma natureza econômica daqueles listados acima, quando negociados no exterior, desde que sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

São exemplos de operação de Baixo Risco: ações negociadas na bolsa de valores; títulos públicos e títulos privados de empresas com grau de investimento e negociados em mercados organizados, dentre outros.

Médio Risco.

As operações classificadas com potencial de Médio Risco acontecem em ambientes de negociação com menor regulação, podem envolver ativos de complexa precificação e com pouco histórico de negociação, de forma que a disparidade de preços frente ao histórico não possa ser aferida com grau de certeza, além de envolverem contraparte que não seja pessoa politicamente exposta (nos termos da lei) ou que apresente algum risco significativo de lavagem de dinheiro, conforme Resolução CVM 50. São exemplos de operação de Médio Risco: títulos privados de empresas com classificação de risco abaixo de grau de investimento negociados em mercados organizados; ativos complexos negociados em balcão não-organizado; dentre outros.

Alto Risco.

As operações classificadas como Alto Risco acontecem em ambientes de negociação com baixa ou nenhuma regulamentação, envolvem ativos de difícil ou extremamente complexa precificação, além de todas as operações que envolverem contrapartes classificadas como pessoas politicamente expostas (nos termos da lei) ou quaisquer outras que possam representar um grau maior de risco de lavagem de dinheiro, conforme a Resolução CVM 50. São exemplos de operações de Alto Risco: quaisquer negociações que envolvam contraparte pessoas politicamente expostas (nos termos da lei), bem como com seus familiares, estreitos colaboradores e pessoas jurídicas de que participem, organizações sem fins lucrativos ou de qualquer outro grau de risco alto para lavagem de dinheiro, conforme Resolução CVM 50; ofertas privadas, ativos de crédito privado fora de ambiente de negociação organizado; ativos de private equity; dentre outros.

Indícios de Atividades Suspeitas

Sem prejuízo da classificação do risco realizada pela Maud conforme matriz acima, convém notar que no monitoramento das operações realizadas pela Maud também serão considerados os seguintes indícios de atividades suspeitas:

- realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;
- que evidenciem oscilação significativa em relação ao volume ou frequência de negócios de qualquer das partes envolvidas;
- cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e beneficiários respectivos;
- cujas características e desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelos envolvidos;
- cujo grau de complexidade e risco se afigurem incompatíveis com: (a) o perfil e histórico de negociação da contraparte ou de seu representante; e (b) com o porte e o objeto social do cliente;
- realizadas com a aparente finalidade de gerar perda ou ganho para as quais falte, objetivamente,

fundamento econômico ou legal;

- transferências privadas de recursos e de valores mobiliários sem motivação aparente, tais como: (a) entre contas-correntes de investidores perante o intermediário; (b) de titularidade de valores mobiliários sem movimentação financeira; e (c) de valores mobiliários fora do ambiente de mercado organizado;
- depósitos ou transferências realizadas por terceiros, para a liquidação de operações de cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;
- pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do cliente;
- operações realizadas fora de preço de mercado;
- operações e situações relacionadas a pessoas suspeitas de envolvimento com atos terroristas, com o financiamento do terrorismo, ou com o financiamento da proliferação de armas de destruição em massa, tais como aquelas que envolvam: (a) ativos alcançados por sanções impostas pelas resoluções do CSNU de que trata a Lei nº 13.810, de 8 de março de 2019; (b) ativos alcançados por requerimento de medida de indisponibilidade oriundo de autoridade central estrangeira de que se venha a ter conhecimento; (c) a realização de negócios, qualquer que seja o valor, por pessoas que tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento, conforme o disposto na Lei nº 13.260, 16 de março de 2016; (d) valores mobiliários pertencentes ou controlados, direta ou indiretamente, por pessoas que tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento, conforme o disposto na Lei nº 13.260, de 2016; e (e) movimentação passível de ser associada ao financiamento do terrorismo, conforme o disposto na Lei nº 13.260, de 2016.
- operações com a participação de pessoas naturais, pessoas jurídicas ou outras entidades que residam, tenham sede ou sejam constituídas em países, jurisdições, dependências ou locais: (a) que não aplicam ou aplicam insuficientemente as recomendações do GAFI, conforme listas emanadas por aquele organismo; e (b) com tributação favorecida e submetidos a regimes fiscais privilegiados, conforme normas emanadas pela Receita Federal do Brasil.

Todas as operações que envolvam quaisquer dos indícios acima elencados, independentemente de terem sido classificadas como de Baixo Risco, Médio Risco ou Alto Risco deverão ser comunicadas ao Diretor de Compliance.

Monitoramento

As operações serão supervisionadas de acordo com sua classificação por grau de risco. As métricas para a classificação de investidores, produtos e serviços prestados pela Maud que deverão permitir defini-los como baixo, médio ou alto risco, serão determinadas anualmente pelo Diretor de Compliance.

No entanto, mesmo nos casos em que o monitoramento estiver enquadrado como de baixo risco, qualquer tipo de atividade suspeita que seja identificada deverá ser reportada à autoridade competente.

Em relação ao monitoramento de investidores em relação aos quais a Maud não possui relacionamento direto por não realizar atividade de distribuição, no limite de suas atribuições, a Maud deverá:

(i) considerar, para fins da abordagem baseada em risco de LDFTP, a política de PLDFTP e as respectivas regras, procedimentos e controles internos de outras instituições responsáveis pelo cadastro de tais investidores;
(ii) realizar intercâmbio de informações com as áreas de controles internos das instituições mencionadas no item "(i)" acima que tenham tal relacionamento direto, observados eventuais regimes de sigilo ou restrição de acesso previstos na legislação;
(iii) monitorar continuamente as operações realizadas em nome desses investidores, considerando as operações ou situações que não dependam da posse dos dados cadastrais, nem tampouco da identificação do beneficiário final, assim como, quando cabível, adotar as providências descritas neste anexo e na política de PLDFT; e
(iv) avaliar a pertinência e a oportunidade de solicitar informações adicionais às instituições mencionadas no item "(i)" acima que tenham relacionamento direto com os investidores, por meio dos mecanismos de intercâmbio a que se refere o item "(ii)" acima, caso aplicáveis, em observância às diretrizes estabelecidas neste anexo e na política de PLDFT.

A Maud realizará o monitoramento com metodologia aprovada pelo Diretor de Compliance e que avalia cada um dos indícios de lavagem de dinheiro citados acima, bem como a faixa de preços dos ativos negociados e o risco das contrapartes. Os resultados do monitoramento serão documentados e arquivados.

A Maud entende que os indicadores acima referenciados estão aptos a mitigar os riscos de lavagem de dinheiro consistentes com as atividades por si desempenhadas.

ANEXO III – Declaração para Contratação de Terceiros

Na capacidade de representante legal da sociedade [incluir nome da sociedade e qualificação], declaro que a sociedade, seus acionistas controladores diretos e indiretos e suas subsidiárias, se existentes, previnem atos de corrupção, fraude, lavagem de dinheiro e financiamento ao terrorismo, e quaisquer outros atos que podem ser nocivos à administração pública nacional ou estrangeira e à ordem econômica. Ademais, na medida do quanto legal e contratualmente permitido, neste ato me comprometo a reportar qualquer violação que venha ser do conhecimento da [sociedade] ou do meu conhecimento.

[Local e data]

_____