



MAKALU GESTÃO DE RECURSOS LTDA.

MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

Outubro/2025

ÍNDICE

INTRODUÇÃO	4
1.1. Sumário	4
1.2. Aplicabilidade do Manual	4
1.3. Ambiente Regulatório	4
1.4. Termo de Compromisso	5
POLÍTICA DE COMPLIANCE	6
1. Introdução	6
1.1 Responsabilidades e Obrigações	6
1.2 Garantia de Independência.....	9
1.3 Dúvidas ou ações contrárias aos princípios e normas do Manual	9
1.4 Acompanhamento das Políticas descritas neste Manual	9
1.5 Sanções (“ <i>Enforcement</i> ”)	10
1.6 Dever de Reportar	11
2. Políticas de Confidencialidade	11
2.1. Sigilo e Conduta	11
3. Políticas de Segregação das Atividades e Conflito de Interesses	13
3.1. Segregação de Atividades	13
3.2. Conflito de Interesses	16
4. Políticas de Treinamento	17
4.1 Treinamento e Processo de Reciclagem.....	17
4.2 Implementação e Conteúdo.....	18
5 Políticas de Segurança e Segurança Cibernética	18
5.1 Identificação de Riscos (<i>risk assessment</i>)	18
5.2 Ações de Prevenção e Proteção	19
5.3 Monitoramento e Testes.....	23
5.4 Plano de Identificação e Resposta	24
5.5 Arquivamento de Informações	25
5.6 Propriedade Intelectual.....	25
5.7 Treinamento	26
5.8 Revisão da Política.....	26
6 Política de Sustentabilidade	26
7 Política Anticorrupção	26

7.1 Introdução	26
7.2 Abrangência das Normas de Anticorrupção	27
7.3 Definição	27
7.4 Normas de Conduta	28
7.5 Proibição de Doações Eleitorais	28
7.6 Relacionamento com Agentes Públicos	29
POLÍTICA DE CERTIFICAÇÃO	30
VIGÊNCIA E ATUALIZAÇÃO	33
ANEXO I	34
ANEXO II	35
ANEXO III	39
ANEXO IV	40
ANEXO V	41

INTRODUÇÃO

1.1. Sumário

Este Manual de Regras, Procedimentos e Controles Internos (“Manual”), elaborado em conformidade com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014, na Resolução CVM nº 21 de 25 de fevereiro de 2021, conforme alterada (“Res CVM 21”), demais orientações da CVM, no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros (“Código ANBIMA de ART”), e no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada (“Código ANBIMA de Certificação”), tem por objetivo estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança (“Colaboradores”) com a **MAKALU GESTÃO DE RECURSOS LTDA.** (“Gestora ou Makalu”), tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Na busca incessante da satisfação dos clientes, a Gestora atua com total transparência, respeito às leis, normas e aos demais participantes do mercado financeiro e de capitais.

Dessa forma, o presente Manual reúne as diretrizes que devem ser observadas pelos Colaboradores no desempenho da atividade profissional, visando ao atendimento de padrões éticos cada vez mais elevados. Este documento reflete a identidade cultural e os compromissos que a Gestora assume nos mercados em que atua.

A Gestora e seus Colaboradores não admitem e repudiam qualquer manifestação de preconceitos relacionados à origem, etnia, religião, classe social, sexo, deficiência física ou qualquer outra forma de preconceito que possa existir.

A Gestora mantém versões atualizadas do presente Manual em seu website (“<https://www.makalupartners.com>”), juntamente com os seguintes documentos: (i) Formulário de Referência, conforme Anexo D da Resolução CVM 21; (ii) Política de Gestão de Risco; (iii) Política de Rateio e Divisão de Ordens; e (iv) Política de Exercício de Direito de Voto.

1.2. Aplicabilidade do Manual

O presente Manual aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na Gestora, possam ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.3. Ambiente Regulatório

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de recebimento e compromisso

constante do **Anexo I** a este Manual (“Termo de Recebimento e Compromisso”), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Gestora foram apontadas no **Anexo IV** do presente Manual.

1.4. Termo de Compromisso

Todo Colaborador, ao receber este Manual, firmará o Termo de Recebimento e Compromisso. Por meio desse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual e com as normas, princípios, conceitos e valores aqui contidos; comprometendo-se a zelar pela aplicação das normas de *compliance* e princípios nele expostos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da Gestora, deverá ser levado para apreciação do Diretor de *Compliance, Risco e PLD* abaixo definido, de acordo com os procedimentos estabelecidos neste Manual. Competirá ao Diretor de *Compliance, Risco e PLD* aplicar as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar o Diretor de *Compliance, Risco e PLD* sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Gestora, bem como zelar pela reputação da empresa. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de *Compliance, Risco e PLD*, o Colaborador deverá informar diretamente aos demais administradores da Gestora.

POLÍTICA DE COMPLIANCE

1. Introdução

1.1 Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do Sr. **FELIPE REIS CICIARELLI**, inscrito no CPF sob o nº 442.471.708-99, na qualidade de diretor estatutário da Gestora indicado como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora ("Diretor de Compliance, Risco e PLD"), nos termos da Resolução CVM 21.

São obrigações do Diretor de *Compliance, Risco e PLD*:

- (i) Acompanhar as políticas descritas neste Manual;
- (ii) Levar quaisquer pedidos de autorização, orientação ou esclarecimento ou casos de ocorrência, suspeita ou indício de prática que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis à atividade da Gestora para apreciação dos administradores da Gestora;
- (iii) Atender prontamente todos os Colaboradores;
- (iv) Identificar possíveis condutas contrárias a este Manual;
- (v) Centralizar informações e revisões periódicas dos processos de *compliance*, principalmente quando são realizadas alterações nas políticas vigentes ou se o volume de novos Colaboradores assim exigir;
- (vi) Assessorar o gerenciamento dos negócios no que se refere ao entendimento, interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, bem como analisar, periodicamente, as normas emitidas pelos órgãos competentes, como a Comissão de Valores Mobiliários ("CVM") e outros organismos congêneres;
- (vii) Providenciar, quando da sua identificação, as comunicações necessárias às autoridades competentes as operações tidas como suspeitas no âmbito da Política de Combate e Prevenção à Lavagem de Dinheiro da Gestora, bem como providenciar relatório **anual** contemplando todas as comunicações realizadas, ou então providenciar a comunicação **anual** negativa às autoridades competentes;
- (viii) Encaminhar aos órgãos de administração da Gestora, até o **último dia útil do mês de abril** de cada ano, relatório referente ao ano civil imediatamente anterior

à data de entrega, contendo: **(a)** as conclusões dos exames efetuados; **(b)** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e **(c)** a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; devendo referido relatório permanecer disponível à CVM na sede da Gestora;

- (ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes deste Manual ou de outros documentos que vierem a ser produzidos para este fim, elaborando sua revisão periódica;
- (x) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio dos treinamentos periódicos previstos neste Manual;
- (xi) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de *compliance* previstos neste Manual ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;
- (xii) Garantir o sigilo de eventuais denunciadores de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;
- (xiii) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;
- (xiv) Aplicar as eventuais sanções aos Colaboradores, conforme definido pelo Comitê de *Compliance* e Risco;
- (xv) Assegurar que os Colaboradores não negociem, em nome próprio ou de terceiros, valores mobiliários e ativos financeiros que não estejam em conformidade com as determinações da Política de Investimentos Pessoais da Makalu;
- (xvi) Ministrando treinamentos a todos os Colaboradores, no mínimo, **anualmente**, promovendo a ampla divulgação dos Manuais e Políticas da Makalu a todos os Colaboradores e abrangendo todos os temas abordados no Programa de Treinamento delineado neste Manual;
- (xvii) Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como “conflitos de interesse” pessoais e profissionais. Esses conflitos podem acontecer, inclusive, mas não limitadamente, em situações que envolvam:

- Investimentos pessoais;
- Transações financeiras com clientes fora do âmbito da Gestora;
- Recebimento de favores/presentes de administradores e/ou sócios de companhias investidas, fornecedores ou clientes;
- Análise financeira ou operação com empresas cujos sócios, administradores ou funcionários, o Colaborador possua alguma relação pessoal;
- Análise financeira ou operação com empresas em que o Colaborador possua investimento próprio; ou
- Participações em alguma atividade política.

Todo e qualquer Colaborador que souber de informações ou situações em andamento, que possam afetar os interesses da Gestora, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos neste Manual, deverá informar o Diretor de *Compliance*, *Risco* e *PLD* para que sejam tomadas as providências cabíveis.

O Diretor de *Compliance*, *Risco* e *PLD* poderá contar, ainda, com outros Colaboradores para as atividades e rotinas de *compliance* e de risco, com as atribuições a serem definidas caso a caso, a depender da necessidade da Gestora em razão de seu crescimento e de acordo com a senioridade do Colaborador.

Ademais, a Gestora possuirá também um Comitê de *Compliance* e Risco, que será composto pelo Diretor de *Compliance*, *Risco* e *PLD*, pelos demais membros da Área de *Compliance* e Risco (abaixo definida) e pelo Diretor de Investimentos (abaixo definido), e deverá averiguar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos da Gestora, entre outros assuntos relacionados à área conforme descrito abaixo, além dos demais assuntos pertinentes à gestão de risco das carteiras, conforme Política de Gestão de Risco da Gestora. A Gestora destaca que o Diretor de Investimentos participará do Comitê de *Compliance* e Risco apenas para fins de reporte.

São atribuições do Comitê de *Compliance* e Risco da Gestora relacionadas a este Manual:

- Analisar eventuais situações do Diretor de *Compliance*, *Risco* e *PLD* sobre as atividades e rotinas de *compliance*;
- Revisar as metodologias e parâmetros de controle existentes; e
- Analisar eventuais casos de infringência das regras descritas neste Manual, nas demais políticas e manuais internos da Gestora, das regras contidas na

regulamentação em vigor, ou de outros eventos relevantes e definir sobre as sanções a serem aplicadas.

As reuniões do Comitê de *Compliance* e Risco serão realizadas **semestralmente**, ou sob demanda, e suas deliberações serão consignadas em atas registradas na rede da Gestora.

1.2 Garantia de Independência

Os Colaboradores que desempenharem as atividades de risco e *compliance* formarão a Área de *Compliance* e Risco, sob a coordenação do Diretor de *Compliance, Risco e PLD*, sendo certo que a Área de *Compliance* e Risco exerce suas atividades de forma completamente independente das outras áreas da Gestora e poderá exercer seus poderes e autoridade com relação a qualquer Colaborador.

1.3 Dúvidas ou ações contrárias aos princípios e normas do Manual

Este Manual possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da Gestora, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de *compliance* e princípios que orientam as ações da Gestora.

Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, também é imprescindível que se busque auxílio imediato junto ao Diretor de *Compliance, Risco e PLD*, para obtenção de orientação mais adequada.

Mesmo que haja apenas a suspeita de uma potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da Gestora, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Gestora e reforçar os seus princípios éticos.

Para os fins do presente Manual, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de *Compliance, Risco e PLD*, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições deste Manual e das demais normas aplicáveis às atividades da Gestora, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de *Compliance, Risco e PLD*, exclusivamente por meio de e-mail.

1.4 Acompanhamento das Políticas descritas neste Manual

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, que cheguem ao conhecimento do Diretor de *Compliance, Risco e PLD*, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de *Compliance, Risco e PLD*

utilizará os registros e sistemas de monitoramento eletrônico referidos neste Manual para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelo Diretor de *Compliance, Risco e PLD*, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de *Compliance, Risco e PLD* julgue necessário.

O Diretor de *Compliance, Risco e PLD* poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

A Gestora realizará inspeções com periodicidade **trimestral**, a cargo do Diretor de *Compliance, Risco e PLD*, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual, com base em sistemas de monitoramento eletrônico, para que sejam verificados, dentre outros os arquivos eletrônicos, inclusive e-mails, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Gestora, sendo tal inspeção realizada de forma aleatória.

Adicionalmente, o Diretor de *Compliance, Risco e PLD* deverá ainda verificar rotineiramente os níveis de controles internos e *compliance* junto a todas as áreas da Gestora, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, o Diretor de *Compliance, Risco e PLD* poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

1.5 Sanções (“*Enforcement*”)

A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade Diretor de *Compliance, Risco e PLD*, conforme por definido pelo Comitê de *Compliance* e Risco, garantido ao Colaborador, contudo, amplo direito de defesa. Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Gestora, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Gestora, nesse último caso, nos termos do artigo 482 da Consolidação das Leis do Trabalho – CLT, sem prejuízos do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

A Gestora não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a Gestora venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, pode exercer o direito de regresso em face dos responsáveis.

1.6 Dever de Reportar

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos deste Manual deverá reportar, imediatamente, tal acontecimento ao Diretor de *Compliance*, *Risco e PLD*. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. Além disso, todos os comunicados e investigações serão tratados de maneira confidencial, na medida do possível nestas circunstâncias. Contudo, o Colaborador que se omitir de tal obrigação poderá sofrer além de ação disciplinar, demissão por justa causa, conforme regime jurídico.

2. Políticas de Confidencialidade

2.1. Sigilo e Conduta

As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na Gestora, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores deverão ler atentamente e entender o disposto neste Manual, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no **Anexo II** ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no **Anexo IV** deste Manual) e de *compliance* da Gestora.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da Gestora, incluindo:

- a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou

- comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;
- c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Gestora;
 - d) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
 - e) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), informações acerca de demandas judiciais, projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
 - f) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
 - g) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
 - h) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados.

Sem prejuízo da colaboração da Gestora com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de *Compliance, Risco e PLD*, para que este decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading, Dicas* ou *Front-running*.

Insider Trading e “Dicas”

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

Front-running significa a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a Gestora, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de *Compliance*, *Risco* e *PLD*, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de *Compliance*, *Risco* e *PLD*, anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável, incluindo eventual demissão por justa causa.

3. Políticas de Segregação das Atividades e Conflito de Interesses

3.1. Segregação de Atividades

Atualmente, no mercado regulado, a Gestora desempenha exclusivamente atividades voltadas para a gestão de carteiras de valores mobiliários, representada pela gestão de fundos de investimento, a qual é exaustivamente regulada pela CVM.

Tal atividade exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de administração de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas pela Gestora ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

Neste sentido, a Gestora, sempre que aplicável, assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais objetivando a segregação física de instalações, bem como a segregação lógica, garantindo inclusive a correta e segregada utilização de

equipamentos e informações entre a Gestora e empresas responsáveis por diferentes atividades prestadas no mercado de capitais.

Todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Gestora, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de gestão de carteiras de valores mobiliários, desenvolvidas pela Gestora, não deverão ser divulgadas a terceiros sem a prévia e expressa autorização do Diretor de *Compliance, Risco e PLD*.

Neste sentido, todos os Colaboradores deverão respeitar as regras e segregações estabelecidas neste Manual e guardar o mais completo e absoluto sigilo sobre as informações que venham a ter acesso em razão do exercício de suas atividades. Para tanto, cada Colaborador, ao firmar o Termo de Compromisso, atesta expressamente que está de acordo com as regras aqui estabelecidas e, por meio da assinatura do Termo de Confidencialidade, abstém-se de divulgar informações confidenciais que venha a ter acesso.

A Gestora deve exercer suas atividades com lealdade e boa-fé em relação aos seus clientes, evitando práticas que possam ferir a relação fiduciária com eles mantida.

Portanto, quando do exercício de suas atividades, os Colaboradores devem atuar com a máxima lealdade e transparência com os clientes. Isso significa, inclusive, que diante de uma situação de potencial conflito de interesses, a Gestora deverá informar ao cliente que está agindo em conflito de interesses e as fontes desse conflito, sem prejuízo do dever de informar após o surgimento de novos conflitos de interesses.

A coordenação das atividades de gestão de carteiras de valores mobiliários da Gestora é uma atribuição do Sr. **LUIZ HUMBERTO GUIMARÃES DE CASTRO PRADO**, inscrito no CPF/MF sob n.º 921.435.471-53, diretor estatutário da Gestora, conforme indicado em seu Formulário de Referência ("Diretor de Investimentos").

Cabe destacar que a Makalu se encontra sob controle comum da Makalu Finanças e Estratégia Ltda., inscrita no CNPJ sob o nº 24.263.137/0001-05 ("Makalu Consultoria"), empresa que atua no segmento de consultoria de operações de finanças corporativas, com foco em *distressed assets* de natureza judicial (consultoria não regulada – não abrangida pela Resolução CVM nº 19/2021), sendo, portanto, de segmento similar ao dos fundos de investimentos a serem geridos pela Makalu, sendo que parte dos colaboradores da Makalu Consultoria também desempenha funções na Makalu, tanto na área de gestão de recursos quanto nas áreas de compliance e risco.

A Makalu ressalta que, nos termos da regulamentação em vigor, a imposição da segregação de forma compulsória é apenas e tão somente devida entre a área responsável pela administração de carteiras de valores mobiliários e as áreas

responsáveis pela intermediação e distribuição de valores mobiliários, atividades estas não desempenhadas pela Makalu e Makalu Consultoria.

Com efeito, apesar de não haver a necessidade de segregação das atividades, quer seja pelo texto literal da norma, quer seja pelo conceito amplo de risco de atos ilícitos, fato é que a norma não veda a existência de potenciais conflitos de interesse, mas obriga que, na existência de potenciais conflitos de interesse, os participantes de mercado criem mecanismos de mitigação e que os potenciais conflitos de interesse sejam, portanto, devidamente endereçados para a ciência da CVM, dos investidores e das empresas atuantes no mercado que venham a se relacionar com a Makalu.

Em razão das atividades exercidas pela Makalu Consultoria e pela Makalu, e considerando os dispositivos constantes da regulamentação em vigor, não há atualmente segregação física entre tais empresas, havendo apenas a segregação de seus sistemas e pastas de acesso no diretório, sendo que todas as obrigações regulatórias estão sendo devidamente atendidas e que, ademais, os potenciais conflitos de interesse e a forma de seu tratamento constam do item 3.2 abaixo.

Por fim, a Makalu informa que, apesar da existência de colaboradores em comum entre as empresas, como mencionado acima, fato é que aqueles que tão somente atuam na Makalu Consultoria, em decorrência da segregação sistêmica das instituições, não possuem qualquer acesso às informações e aos documentos da Makalu.

Atuação do Diretor de Compliance

A Makalu ressalta que o Diretor de *Compliance*, Risco e PLD não atuará em funções de negócio ou em qualquer atividade que limite a sua independência, na Makalu ou fora dela, nos termos da regulamentação em vigor, de forma a possibilitar a integral identificação e mitigação de potenciais conflitos de interesse, e garantir a sua devida atuação regulatória perante a CVM e os investidores das carteiras de valores mobiliários sob gestão da Makalu.

Disposições Adicionais

Ademais, a Makalu não contratará, num primeiro momento, terceiros para a prestação de serviços de *back office* e análise de valores mobiliários, contando apenas com seu departamento técnico para tanto.

No entanto, caso a Makalu venha a contratar terceiros para a prestação de serviços de *back office* e análise de valores mobiliários, a Makalu adotará regras e procedimentos internos capazes de assegurar a completa segregação de funções, atividades e responsabilidades relacionadas com a administração de carteira de valores mobiliários.

Caso a Makalu contrate os serviços mencionados acima, todos os Colaboradores que tiverem suas atividades profissionais relacionadas com a gestão de carteira de títulos e valores mobiliários serão alocados em local diverso dos demais prestadores de serviços,

incluindo acesso exclusivo por meio de ponto eletrônico, utilização de instalações físicas totalmente independentes e segregadas, disponibilização de linhas telefônicas específicas e diretório de rede privativo e restrito, acessível somente mediante login e senha individuais.

Por outro lado, a Makalu contratará, a qualquer momento, terceiros que não estejam ligados à sua atividade principal.

3.2. Conflito de Interesses

Conflitos de interesse são situações decorrentes do desempenho das funções de determinado Colaborador, nas quais os interesses pessoais de tal Colaborador possam ser divergentes ou conflitantes com os interesses da Gestora e/ou entre os interesses diferentes de dois ou mais de seus clientes, para quem a Gestora tem um dever para cada um ("Conflito de Interesses").

O Colaborador tem o dever de agir com boa-fé e de acordo com os interesses dos investidores com o intuito de não ferir a relação fiduciária com o cliente. Para tal, o Colaborador deverá estar atento para uma possível situação de conflito de interesses, e sempre que tal situação ocorrer deverá informar, imediatamente, o Diretor de *Compliance, Risco e PLD* sobre sua existência e abster-se de consumir o ato ou omissão originador do Conflito de Interesse até decisão em contrário.

Em razão das atividades atualmente desempenhadas pela Gestora no mercado regulado, conforme indicado no item anterior, a Gestora entende não existir qualquer conflito de interesses potencial ou efetivo a ser aqui tratado.

Não obstante a Makalu não desempenhar atividade adicional no mercado regulado além da própria atividade de gestão de recursos, a Makalu ressalta, conforme informado acima, a respeito da atuação da Makalu Consultoria, que atua no segmento de consultoria de operações de finanças corporativas com foco em *distressed assets* de natureza judicial, sendo, portanto, de segmento similar ao dos fundos de investimentos a serem geridos pela Makalu.

Neste sentido, relativamente ao exposto no parágrafo acima, de forma a tratar potencial ou efetivo conflito de interesses entre a prestação de serviços pela Makalu e pela Makalu Consultoria, as seguintes medidas deverão ser tomadas, sem prejuízo do dever de fidúcia contínuo da Makalu e da atuação contínua com boa-fé:

- (i) antes da realização de novos investimentos pelos fundos sob gestão da Makalu em *distressed assets*, o Diretor de Investimentos deverá questionar formalmente o Diretor de *Compliance, Risco e PLD* quanto à eventual prestação de serviços pela Makalu Consultoria para os detentores e/ou emissores dos ativos alvos dos fundos sob gestão da Makalu, para identificar se tal assessoria poderia representar ou desencadear em qualquer potencial conflito de interesses frente ao eventual investimento a ser realizado pelos fundos sob gestão da Makalu;

- (ii) os créditos originados, cedidos ou de outra forma estruturados pela Makalu Consultoria ou por outras partes relacionadas à Makalu, direta ou indiretamente, não poderão ser adquiridos pelos fundos de investimento sob gestão da Makalu;
- (iii) sem prejuízo do disposto acima, caso por qualquer razão a Makalu venha a acreditar que o investimento por fundos sob sua gestão em determinado ativo possa representar potencial conflito de interesses, a matéria deverá ser levada ao Comitê de Compliance e Risco, e, conforme necessidade, deverá ser solicitado ao administrador dos fundos a convocação de assembleia geral de cotistas para deliberação a respeito da matéria relevante e de comum interesse mencionada; e
- (iv) os fundos sob gestão da Makalu sempre terão preferência sobre a aquisição e demais operações de investimento e desinvestimento em *distressed assets* identificados como oportunidades de investimento pela Makalu Consultoria, salvo em casos de impossibilidade da operação pela política de investimento dos fundos, assim como nos casos de insuficiência de patrimônio dos fundos para o investimento.

Com isso, a Makalu enfatiza que todas as obrigações regulatórias estão sendo devidamente atendidas em razão de: (i) possuir manuais com informações claras e objetivas, e controles adequados; e (ii) possuir política de treinamento para todos os seus colaboradores, de forma a (a) assegurar o bom uso de instalações, equipamentos e informações comuns, (b) preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas, e (c) restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

4. Políticas de Treinamento

4.1 Treinamento e Processo de Reciclagem

A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, especialmente aqueles que tenham acesso à Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Assim que cada Colaborador for contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Gestora e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Neste sentido, a Gestora adota um programa de reciclagem **anual** dos seus Colaboradores, à medida que as normas, princípios, conceitos e valores contidos neste Manual sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

4.2 Implementação e Conteúdo

A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de *Compliance, Risco e PLD* e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Gestora, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas neste Manual (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo IV** deste Manual.

O Diretor de *Compliance, Risco e PLD* poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.

5 Políticas de Segurança e Segurança Cibernética

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Gestora e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito e com monitoramento com câmera de segurança. As estações de trabalho serão fixas, com notebooks seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Diretor de *Compliance, Risco e PLD*, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

5.1 Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos

e externos que precisam de proteção:

- **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- **Sistemas:** informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e
- **Governança da Gestão de Risco:** a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- **Malware** – softwares desenvolvidos para corromper computadores e redes (tais como: *Vírus, Cavalo de Troia, Spyware e Ransomware*);
- **Engenharia social** – métodos de manipulação para obter informações confidenciais (*Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal*);
- **Ataques de DDoS (*distributed denial of services*) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- **Invasões (*advanced persistent threats*):** ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima e, no que aplicável, no Plano de Contingência e Continuidade dos Negócios da Gestora, há a avaliação e definição do plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

5.2 Ações de Prevenção e Proteção

Após a identificação dos riscos, a Gestora adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta:

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, a Área de *Compliance* e Risco deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Ademais, fica terminantemente proibido que os Colaboradores discutam remotamente Informações Confidenciais.

Cada Colaborador será responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora.

A Gestora mantém arquivo em nuvem e o descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores estarão proibidos de utilizar pen-drivers, fitas, discos ou quaisquer outros meios externos à rede da Gestora,

exceto mediante a aprovação do Diretor de *Compliance, Risco e PLD*. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pelos administradores da Gestora.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gestora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora.

A visualização de *sites, blogs, fotologs, webmails*, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

- Acesso Escalonado do Sistema

O acesso como “administrador” de área de *desktop* é limitado aos usuários aprovados pelo Diretor de *Compliance, Risco e PLD* e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Gestora necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação

- Senha e Login

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via *webmail*, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas **trimestralmente**, conforme aviso fornecido pelo responsável pela área de informática. Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

- Uso de Equipamentos e Sistemas

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de *Compliance, Risco e PLD*.

- Acesso Remoto

A Gestora permite o acesso remoto pelos Colaboradores de forma escalonada, no que se refere a rede, diretório e e-mail, de acordo com funções e senioridade dos mesmos e mediante aprovação do Diretor de *Compliance, Risco e PLD*.

O acesso remoto será realizado através do Dropbox Professional, com criptografia Advanced Encryption Standard (AES) de 256-bit. Para proteger os dados em trânsito entre os aplicativos do Dropbox (para desktop, dispositivos móveis, API ou na web), o Dropbox usa criptografia Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para transferência de dados, criando um túnel seguro protegido por padrões avançados de criptografia AES de 128-bits ou superior. Todo Colaborador deverá passar por autenticação para se conectar à rede.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter *softwares* de proteção contra *malware*/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de *Compliance, Risco e PLD* acerca de qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

- Controle de Acesso

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da Gestora.

O acesso ao Data-Center é restrito ao Diretor de *Compliance, Risco e PLD* ou por pessoa previamente autorizada pelo Diretor de *Compliance, Risco e PLD*. O acesso será controlado e contará com monitoramento 24 horas por dia com câmera de gravação.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

- *Firewall, Software, Varreduras e Backup*

A Gestora utiliza *hardwares* de *firewall* com estrutura de redundância, projetados para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de *Compliance, Risco e PLD* é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A Gestora mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus, worms, spyware*). Serão conduzidas varreduras constantes para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Gestora.

A Gestora utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O Diretor de *Compliance, Risco e PLD* é responsável por patches regulares nos sistemas da Gestora.

A Gestora mantém e testa regularmente medidas de *backup* consideradas apropriadas pelo Diretor de *Compliance, Risco e PLD*. As informações da Gestora são atualmente objeto de *backup diário* com o uso de computação na nuvem pelo sistema Dropbox Professional. Os dados de e-mail e comunicação estarão em padrão da plataforma G-Suite desenvolvida pelo Google e possui os certificados mais respeitados do mundo, tais como: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2/3, FedRAMP e PCI DSS, que assegura elevado nível de controle de identidade, gerenciamento de dispositivos e proteção e inteligência sobre os dados.

5.3 Monitoramento e Testes

O Diretor de *Compliance, Risco e PLD* (ou pessoa por ele incumbida) adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, **semestral**:

- (i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, *blogs, fotologs, webmails*, entre outros, bem como os e-mails enviados e recebidos;
- (ii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a *desktops*, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de *Compliance, Risco e PLD* poderá adotar medidas adicionais para monitorar

os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

Desta forma, ao realizar os procedimentos acima descritos, o Diretor de *Compliance*, Risco e PLD identificará, caso existam, Colaboradores detentores de informações confidenciais para responsabilização, em caso de vazamento.

5.4 Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de *Compliance*, Risco e PLD prontamente. O Diretor de *Compliance*, Risco e PLD determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de *Compliance*, Risco e PLD determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Diretor de *Compliance*, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

- (i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
- (ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- (iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
- (iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- (v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
- (vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais

de fundo de investimento sob gestão da Gestora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

- (vii) Determinação do responsável (ou seja, a Gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de *Compliance*, Risco e PLD após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

5.5 Arquivamento de Informações

De acordo com o disposto neste Manual, os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 18 da Resolução CVM 21.

5.6 Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gestora, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora, salvo se autorizado expressamente pela Gestora e ressalvado o disposto abaixo.

Caso um Colaborador, **ao ser admitido**, disponibilize à Gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Gestora, o Colaborador deverá assinar declaração nos termos do **Anexo V** ao presente Manual, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

5.7 Treinamento

O Diretor de *Compliance*, Risco e PLD organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de *compliance* (conforme descrito nos itens 1.4 e 4 acima).

5.8 Revisão da Política

O Diretor de *Compliance*, Risco e PLD realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética a cada **24 (vinte e quatro) meses**, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

6 Política de Sustentabilidade

A Gestora deve sempre buscar adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, incluindo, mas não se limitando a: (a) utilização de papel reciclável para impressão de documentos; (b) utilização de refil de cartuchos e toners para impressão; (c) separação do material reciclável para fins de coleta seletiva de lixo; (d) utilização de lâmpadas de baixo consumo energético; e (e) incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Colaboradores, como transportes coletivos, caronas ou bicicletas.

Além disso, a Gestora incentiva seus Colaboradores a adotar postura semelhante no dia a dia de suas atividades, por exemplo: (a) evitar imprimir e-mails e arquivos eletrônicos, exceto se necessário; (b) optar por utilizar canecas ou copos reutilizáveis; (c) desligar os computadores todos os dias ao final do expediente; (d) apagar as luzes das salas ao sair; e (e) desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

7 Política Anticorrupção

7.1 Introdução

A Gestora está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção").

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Gestora e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

7.2 Abrangência das Normas de Anticorrupção

As Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira 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 e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados “agentes públicos” para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

7.3 Definição

Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

- I. I prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
- II. II comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;
- III. III comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
- IV. IV no tocante a licitações e contratos:

- a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
- b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
- c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
- d) fraudar licitação pública ou contrato dela decorrente;
- e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
- f) 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
- g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

V. V dificultar atividade de investigação ou fiscalização de 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.

7.4 Normas de Conduta

É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização prévia do Diretor de *Compliance*, Risco e PLD.

Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

7.5 Proibição de Doações Eleitorais

A Gestora não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, estes têm a obrigação de seguir estritamente a legislação vigente, podendo realizar doações, desde que respeitadas as normas de Anticorrupção.

7.6 Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências (“Audiências”) com agentes públicos, sejam elas internas ou externas, a Gestora será representada por, ao menos, 2 (dois) Colaboradores, salvo no caso de outorga de procurações específicas com poder individualizado que permitam atuações isoladas, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a Gestora contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Gestora deverão elaborar relatórios de tais Audiências, e os apresentar ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

POLÍTICA DE CERTIFICAÇÃO

1. Introdução

A Gestora aderiu e está sujeita às disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada (“Código ANBIMA de Certificação”), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

2. Atividades Elegíveis e Critérios de Identificação

Tendo em vista a atuação da Gestora como gestora de recursos de terceiros, foi identificado, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA (“CGA e CGE”) é a única certificação pertinente às suas atividades, sendo que a CGA aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento em fundos de ações, renda fixa, multimercados e cambiais, e a CGE aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento em fundos de índices, imobiliários e de direitos creditórios.

Nesse sentido, a Gestora definiu que apenas o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Investimentos, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA e/ou CGE.

Colaboradores que não tenham CGA e/ou CGE (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Art. 17 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Gestora sem a aprovação prévia do Diretor de Investimentos, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Em complemento, a Gestora destaca que a CGA e CGE é certificação pessoal e intransferível. Caso o Colaborador esteja exercendo a atividade elegível de CGA e/ou CGE na Gestora, conforme acima indicada, e a certificação não esteja vencida a partir do vínculo do Colaborador com a Gestora, o prazo de validade da certificação CGA e CGE será indeterminado, enquanto perdurar o seu vínculo com a Gestora. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGA e/ou CGE na Gestora, a validade da certificação será de 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixou de exercer a atividade elegível de CGA e/ou CGE.

Desse modo, a Gestora assegurará que os Colaboradores que atuem nas atividades elegíveis participem do procedimento de atualização de suas respectivas certificações, de modo que a certificação obtida esteja devidamente atualizada dentro dos prazos estabelecidos neste Manual e nos termos previstos no Código ANBIMA de Certificação.

3. Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

Contratação

Antes da contratação ou admissão de qualquer Colaborador, o Diretor de *Compliance*, Risco e PLD deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação.

O Diretor de Investimentos deverá esclarecer ao Diretor de *Compliance*, Risco e PLD se Colaboradores que integrarão a Equipe de Gestão terão ou não alçada/poder discricionário de decisão de investimento.

Caso seja identificada a necessidade de certificação, o Diretor de *Compliance*, Risco e PLD deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

Alteração de Funções

Ainda, o Diretor de Investimentos deverá contatar e informar o Diretor de *Compliance*, Risco e PLD sempre que houver algum tipo de alteração nos cargos e funções dos Colaboradores que integram a Equipe de Gestão, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Desligamento

O Diretor de *Compliance*, Risco e PLD também deverá checar se Colaboradores que estejam se desligando da Gestora estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Gestora.

Prazo de Atualização

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer **até o último dia útil do mês subsequente à data do evento** que deu causa a atualização, nos termos do Art. 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de *Compliance*, Risco e PLD, conforme disposto abaixo.

4. Rotinas de Verificação

Trimestralmente, o Diretor de *Compliance*, Risco e PLD deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código ANBIMA de Certificação.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pelo Diretor de *Compliance*, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Investimentos por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível

sem a certificação pertinente ou com a certificação vencida, o Diretor de *Compliance*, Risco e PLD deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, **anualmente** deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de compliance.

Por fim, serão objeto do treinamento **anual** de compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Gestora, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros da Equipe de Gestão de recursos, reforçando que somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Gestora, devendo os demais buscar aprovação junto ao Diretor de Investimentos; (iii) treinamento direcionado aos Colaboradores da Área de *Compliance* e Risco, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do art. 9º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

Os profissionais já certificados, caso deixem de ser Colaboradores da Gestora, deverão assinar a documentação prevista no Anexo a este Manual denominado “Termo de Afastamento”, comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do Anexo aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado **anualmente**, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	Versão	Responsável
Novembro de 2020	1ª	Diretor de <i>Compliance, Risco e PLD</i>
Outubro de 2021	2ª	Diretor de <i>Compliance, Risco e PLD</i>
Outubro de 2022	3ª	Diretor de <i>Compliance, Risco e PLD</i>
Outubro de 2023	4ª	Diretor de <i>Compliance, Risco e PLD</i>
Outubro de 2024	5ª	Diretor de <i>Compliance, Risco e PLD</i>
Outubro de 2025	6ª e Atual	Diretor de <i>Compliance, Risco e PLD</i>

ANEXO I
TERMO DE RECEBIMENTO E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, DECLARO para os devidos fins:

- (i) Ter recebido, na presente data, o Manual de Regras, Procedimentos e Controles Internos atualizado ("Manual") da **MAKALU GESTÃO DE RECURSOS LTDA.** ("Gestora");
- (ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes no Manual;
- (iii) Estar ciente de que o Manual como um todo passa a fazer parte dos meus deveres como Colaborador da Gestora, incorporando-se às demais regras internas adotadas pela Gestora; e
- (iv) Estar ciente do meu compromisso de comunicar ao Diretor de *Compliance, Risco e PLD* da Gestora qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas neste Manual.

[local], [data].

[COLABORADOR]

ANEXO II TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, doravante denominado Colaborador, e **MAKALU GESTÃO DE RECURSOS LTDA.**, inscrita no CNPJ sob o nº 37.336.862/0001-08 ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios FUNDOS, incluindo:

- a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento geridos pela Gestora;
- c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento geridos pela Gestora;
- d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
- e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
- f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
- g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à

Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

- 2.1. O Colaborador se obriga a, durante a vigência deste Termo e pelo prazo de 3 (três) anos contados após sua rescisão ou por outros prazos assumidos em decorrência desta relação, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, “*Insider Trading*”, “*Dicas*” e “*Front Running*”, seja atuando em benefício próprio, da Gestora ou de terceiros.
- 2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.
3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando desde já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.
 - 3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.
 - 3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.
4. O Colaborador reconhece e toma ciência que:
 - (i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[local], [data].

[COLABORADOR]

MAKALU GESTÃO DE RECURSOS LTDA.

Testemunhas:

1. _____

Nome:

CPF:

2. _____

Nome:

CPF:

ANEXO III
PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DA
MAKALU GESTORA DE RECURSOS LTDA.

1. Resolução CVM N° 175/22
2. Resolução CVM N° 21/21
3. Resolução CVM N° 50/21
4. Ofício-Circular/CVM/SIN/N° 05/2014
5. Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros
6. Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada
7. Lei 9.613/98, conforme alterada

Data Base: outubro/2025

ANEXO IV
TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____ (“Colaborador”), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **MAKALU GESTÃO DE RECURSOS LTDA.** (“GESTORA”), nesta data, dos documentos contidos no *pen drive* da marca [•], número de série [•] (“Documentos”), bem como sua futura utilização pela Gestora, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no *pen drive* da marca [•], número de série [•], que ficará com a Gestora e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

[•], [•] de [•] de [•].

[COLABORADOR]

**ANEXO V
TERMO DE AFASTAMENTO**

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **MAKALU GESTÃO DE RECURSOS LTDA.**, inscrita no CNPJ sob o nº 37.336.862/0001-08 (“GESTORA”) por prazo indeterminado:

[] até que me certifique pela CGA, no caso da atividade de gestão de recursos de terceiros com alçada/poder discricionário de investimento;

[] ou até que o Conselho de Certificação, nos termos do Art. 17 do Código de Certificação, me conceda a isenção de obtenção da CGA;

[] tendo em vista que não sou mais Colaborador da Gestora;

São Paulo, [---] de [---] de [---].

[COLABORADOR]

MAKALU GESTÃO DE RECURSOS LTDA.

Testemunhas:

1. _____
Nome:
CPF:

2. _____
Nome:
CPF:

Apêndice
Lista dos Arquivos Gravados nos Pen Drives