MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS ("MANUAL")

Aprovada por:
Comitê de Compliance e Risco

ÍNDICE

1. OBJETIVO E APLICABILIDADE 3
2. BASE LEGAL 4
3. AMBIENTE REGULATÓRIO E TERMO DE COMPROMISSO 4
4. POLÍTICAS 5
   - 4.1. Política de Compliance 5
     - a) Responsabilidades e Obrigações 5
     - a) Garantia de Independência 8
     - b) Dúvidas ou ações contrárias aos princípios e normas do Manual 8
     - b) Acompanhamento das práticas descritas nesta Política 9
     - c) Sanções (“Enforcement”) 10
   - 4.2. Política de Confidencialidade 10
     - a) Sigilo e Conduta 10
     - b) Insider Trading e “Dicas” 13
     - c) Front-running 13
     - d) Spoofing 14
   - 4.3. Política de Treinamento 14
     - a) Treinamento Inicial e Processo de Reciclagem 14
     - b) Responsabilidade 15
     - c) Implementação e Conteúdo 15
   - 4.4. Política de Segurança da Informação e Segurança Cibernética 15
     - a) Identificação de Riscos (*risk assessment*) 16
     - b) Ações de Prevenção e Proteção 17
     - c) Monitoramento e Testes 22
     - d) Plano de Identificação e Resposta 23
     - e) Arquivamento de Informações 24
     - f) Propriedade Intelectual 25
     - g) Treinamento 26
     - h) Revisão da Política 26
   - 4.5. Política de Conflito de Interesses 26

a) Objetivos 26
b) Regras de Presentes e Entretenimentos 27
c) Soft Dollar 28
4.6. Política de Sustentabilidade 31
4.7. Política de Anticorrupção 31
a) Introdução e Abrangência das Normas de Anticorrupção 31
b) Definição 32
c) Normas de Conduta 34
d) Proibição de Doações Eleitorais 34
e) Relacionamentos com Agentes Públicos 34
4.8. Política de Certificação 35
a) Introdução 35
b) Atividades Elegíveis e Critérios de Identificação. 35
c) Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA 36
d) Rotinas de Verificação 37
e) Processo de Afastamento 39
5. VIGÊNCIA E ATUALIZAÇÃO 39
ANEXO I 40
ANEXO II 41
ANEXO III 46
ANEXO IV 47
Apêndice 49
ANEXO V 50

1. OBJETIVO E APLICABILIDADE

O presente Manual objetiva estabelecer normas, princípios, conceitos e valores que orientem a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a Gestora, tanto na sua atuação interna

quanto na comunicação com os diversos públicos, visando ao atendimento de padrões éticos cada vez mais elevados.

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.

2. BASE LEGAL

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21/21");
(ii) Resolução da Comissão de Valores Mobiliários ("CVM") nº 62, de 19 de janeiro de 2022 ("Resolução CVM 62/22");
(iii) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Ética ("Código de Ética");
(iv) Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código de AGRT");
(v) Regras e Procedimentos de Certificação vinculadas ao Código de AGRT ("Código ANBIMA de Certificação");
(vi) Lei nº 12.846, de 1º de agosto de 2013 e Decreto nº 11.129, de 11 de julho de 2022 ("Normas de Anticorrupção"); e
(vii) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora.

3. AMBIENTE REGULATÓRIO E TERMO DE COMPROMISSO

Este Manual é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, que, ao receberem o presente Manual, deverão assinar o termo de recebimento e compromisso constante do **Anexo I** a este Manual ("Termo de Recebimento e Compromisso"), a fim de demonstrar que aceitam expressamente as normas, princípios, conceitos e valores aqui estabelecidos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Gestora bem como do completo conteúdo deste Manual. As principais normas aplicáveis às atividades da Gestora constam no **Anexo III** do presente Manual.

4. POLÍTICAS

4.1. Política de Compliance

a) Responsabilidades e Obrigações

A coordenação direta das atividades relacionadas a este Manual é uma atribuição do 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 21/21.

São obrigações da Área de Compliance e Risco, sob a responsabilidade do Diretor de Compliance, Risco e PLD:

(i) Acompanhar as políticas descritas neste Manual;

(ii) Analisar inicialmente e 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 do Comitê de Compliance e Risco 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 CVM e outros organismos congêneres;

(vii) Elaborar relatório **anual** listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de Prevenção à Lavagem de Dinheiro da Gestora, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa da Gestora ("Política de PLDFTP");

(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) Garantir o sigilo de eventuais denunciantes de delitos ou infrações, mesmo quando estes não solicitarem, exceto nos casos de necessidade de testemunho judicial;

(xii) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais;

(xiii) Aplicar as eventuais sanções aos Colaboradores, conforme definido pelo Comitê de Compliance e Risco; e

(xiv) 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.

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 possui também um Comitê de Compliance e Risco, conforme previsto em Regimento interno da Gestora.

a) Garantia de Independência

Os Colaboradores da Área de Compliance e Risco atuam sob a coordenação do Diretor de Compliance, Risco e PLD, e todos exercem suas atividades de forma completamente independente das outras áreas da Gestora.

b) 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.

Toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, Risco e PLD e/ou do Comitê de Compliance e Risco, 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 aplicável ao Diretor de Compliance, Risco e PLD, que submeterá para análise em âmbito de Comitê de Compliance e Risco o ocorrido.

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, que reportará tal conduta para avaliação no âmbito do Comitê de Compliance e Risco. Nenhum Colaborador sofrerá retaliação por comunicar, de boa-fé, violações ou potenciais violações a este Manual. O Colaborador que se omitir de tal obrigação poderá sofrer além de ação disciplinar, demissão por justa causa, conforme regime jurídico.

Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, Risco e PLD, o Colaborador deverá informar diretamente aos demais membros do Comitê de Compliance e Risco da Gestora.

b) Acompanhamento das práticas descritas nesta Política

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, este 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 pela Área de Compliance e Risco, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso a Área de Compliance e Risco julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Gestora.

Ainda, a Área de Compliance e Risco deverá ainda verificar, anualmente, 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.

O Diretor de Compliance, Risco e PLD utilizará as informações obtidas em tais monitoramentos, caso aplicável, para reporte ao Comitê de Compliance e Risco, 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.

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

c) Sanções ("Enforcement")

Responsável pela Definição: Comitê de Compliance e Risco.

Responsável pela Aplicação: Diretor de Compliance, Risco e PLD.

Sanções: Advertência, suspensão, desligamento ou exclusão por justa causa, ou demissão por justa causa, conforme aplicável. A Gestora: (i) poderá ainda pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis; (ii) não assume a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções; e (iii) pode exercer o direito de regresso em face dos responsáveis, caso venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores.

4.2. Política de Confidencialidade

a) Sigilo e Conduta

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 III** 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:

(i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora;
(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora;
(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
(v) 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*), 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;
(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
(viii) 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. Para informações classificadas pela Gestora como Estritamente Confidenciais, sua gravação em diretórios da rede Tenax ou outros tipos de mídia deve ser realizada com criptografia, cujo acesso será permitido somente ao Diretor de Compliance, Risco e PLD, ao Diretor de Investimentos e ao responsável pela Área Administrativa da Tenax, em função de seu contato com dados sensíveis. São consideradas informações Estritamente Confidenciais:

- Listas, dados pessoais e/ou informações sensíveis de qualquer natureza de colaboradores, sócios, clientes, prestadores e serviços, e outras partes relacionadas da Gestora.
- Informações estratégicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias, dados financeiros da Gestora para uso interno, ou resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento.
- Informações sobre investigações regulatórias e/ou de ordem jurídica envolvendo a Gestora, como pessoa jurídica, ou seus colaboradores, sócios, clientes, prestadores e serviços e outras partes relacionadas.
- Quaisquer informações cuja divulgação pública ou vazamento possam causar danos substanciais à Gestora e suas partes relacionadas, sejam eles financeiros, reputacionais e/ou regulatórios.

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 ilícitos como, por exemplo, *Insider Trading*, Dicas ou *Front-running*.

b) Insider Trading e "Dicas"

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, obtida por meio de relacionamento profissional e/ou pessoal em caráter sigiloso, em virtude da confiança entre as partes (informações privilegiadas), 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.

É proibida a prática dos casos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Tenax ou de terceiros.

c) 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 de quaisquer práticas ilícitas, incluindo as 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.

d) Spoofing

Spoofing é a prática abusiva que cria liquidez artificial com ofertas de tamanho fora do padrão do livro de ofertas com o objetivo de influenciar investidores a superar a oferta artificial e gerar negócios do lado oposto do livro. Após o negócio, a liquidez artificial na forma de oferta fora do padrão é cancelada. É proibida a prática de *Spoofing* por qualquer membro da gestora, seja agindo em benefício próprio, da Tenax ou de terceiros. Tal prática encontra-se expressamente vedada conforme disposto pela Resolução CVM nº 62/22.

4.3. Política de Treinamento

a) Treinamento Inicial e Processo de Reciclagem

A Gestora possui um processo de treinamento **inicial** de todos os seus Colaboradores, bem como de reciclagem **anual** dos seus Colaboradores, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

b) Responsabilidade

Área de Compliance e Risco, sob a supervisão do Diretor de Compliance, Risco e PLD, a qual poderá contratar profissionais especializados para conduzirem os treinamentos.

c) Implementação e Conteúdo

Deve 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 e segurança cibernética), bem como aquelas descritas no Código de Ética, na Política de Investimentos Pessoais e na Política de PLDFTP da Gestora e, ainda, as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades, constantes do **Anexo III** deste Manual.

4.4. Política de Segurança da Informação 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. As estações de trabalho serão fixas, com computadores 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 da Área de Compliance e Risco, sob supervisão do Diretor de Compliance, Risco e PLD, que será a responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

a) Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) 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);

(ii) Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias *desenvolvidas* internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

(iii) Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e

(iv) 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:

(i) *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

(ii) Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);

(iii) Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

(iv) Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico; e

(v) Vazamento interno de informações realizada por meio de colaboradores ou terceiros que tenham acesso irregular às informações confidenciais da Gestora.

Com base no acima, a Gestora avalia e define o 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.

b) 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.

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 não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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 estão proibidos de utilizar pen-drives, fitas, discos etc. Neste sentido, são permitidos apenas pen-drives criptografados e previamente cadastrados pela Equipe de Tecnologia da Informação que presta suporte à Gestora ("Equipe de TI").

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pelo Diretor de Compliance, Risco e PLD. Ainda, nenhum Colaborador tem permissão de instalação de programas nos servidores e notebooks da Gestora, ficando esta atribuição exclusiva a Equipe de TI.

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*, *redes sociais*, *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.

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, a todos as funcionalidades necessárias ao regular exercício de sua função.

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 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.

Ainda, todos os acessos externos a Gestora, tais como VPN, e-mail e sistemas exigem duplo fator de autenticação para todos os Colaboradores, de forma a buscar uma maior robustez quanto a segurança da informação da própria Gestora.

- **Controle de Acesso**

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelo Comitê de Compliance e Risco.

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 conta com *Firewall* redundante no escritório, *firewall* na *private cloud*, e 3 (três) soluções distintas de proteção instaladas em todos os notebooks dos Colaboradores, para fins de proteção contra vírus e malwares, não só por reconhecimento por assinatura como por comportamento, bem como detecção de intrusão distribuída e não só nas bordas de rede. 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 **anuais** 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.

c) Monitoramento e Testes

A Área de Compliance e Risco adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, como:

(i) Monitoramento, por amostragem, dos e-mails enviados e recebidos, com base em uma lista pré-definida de palavras-chave;

(ii) Acompanhamento dos e-mails enviados para destinatários externos à instituição. Todos os e-mails destinados a domínios de provedores genéricos ou desconhecidos (como serviços de e-mail gratuitos) devem ser submetidos à aprovação prévia, independentemente do conteúdo. Essa medida garante o controle sobre qualquer informação enviada para esses destinatários. E-mails direcionados a organizações e instituições reconhecidas do mercado financeiro e regulatório estão isentos dessa aprovação, pois são considerados ambientes confiáveis.

A Área de Compliance e Risco poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

d) 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 informado 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 Comitê de Compliance e Risco 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, com base nas decisões do Comitê de Compliance e Risco, conforme o caso, 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.

e) <u>Arquivamento de Informações</u>

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 21/21.

f) 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 IV** 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.

g) Treinamento

A Área de Compliance e Risco, sob supervisão do 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 acima).

h) Revisão da Política

A Área de Compliance e Risco realizará uma revisão desta Política de Segurança da Informação e Segurança Cibernética **anualmente**, 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.

4.5. Política de Conflito de Interesses

a) Objetivos

A presente Política de Conflito de Interesses, traz as diretrizes e orientações cujo objetivo é a prevenção de situações que possam caracterizar conflito de interesses. Os conflitos de interesse ocorrem quando os interesses pessoais, financeiro, familiar, político e profissionais do colaborador e ou sócio se opõe aos princípios, valores e objetivos da Gestora, podendo inclusive gerar prejuízos de qualquer natureza para tanto à Gestora como a qualquer das partes relacionadas.

Ademais, o Conflito pode ocorrer quando um profissional age baseado em interesses alheios aos da Gestora, objetivando benefício, para si próprio ou para terceiros, com ele relacionados. Os conflitos de interessem podem se apresentar em 3 (três) modalidades:

Conflitos reais: Ocorre quando o indivíduo deve decidir entre duas ou mais situações conflituosas, onde é evidente que a decisão se baseou por interesse pessoais contrários aos interesses da Gestora. De modo, que se um terceiro observar a situação, este consegue claramente notar claramente o conflito e que a tomada de decisão ocorreu devido ao interesse particular do envolvido.

Conflitos Potenciais: Se apresenta em situação que pode evoluir e materializar-se em conflito de interesse. Um exemplo prático, seria se um colaborador/sócio, ao decidir alguma situação, não possui conhecimento que existem outras situações que com ela conflitam, porém se um terceiro observar essa situação, verifica que poderia existir um conflito de interesse.

Conflitos Aparentes: Ocorre quando a situação, não se configura em conflito de interesse real, porém um terceiro, pode deduzir que o conflito existe. Neste caso, é necessário investigar, a fim de averiguar se de fato a situação, seria ou não um conflito real.

Neste sentido, conflitos de Interesse reais, potenciais e aparentes, os quais de alguma forma possam colocar a Gestora e pessoas à ela relacionadas, em um nível de risco maior que o normal, devem ser reportados ao nível gerencial apropriado e a Diretoria de Compliance.

b) Regras de Presentes e Entretenimentos

Os Colaboradores devem ter nos sócios exemplos de conduta, não sendo admitida a utilização do respectivo cargo para conseguir favores dos subordinados ou desfrutar de benefícios ilícitos dentro ou fora da empresa.

A Gestora faz distinção entre um “Presente” e “Entretenimento.” Os presentes são itens (ou serviços) de valor que um terceiro fornece a um Colaborador (ou um Colaborador ao terceiro). O entretenimento, por outro lado, contempla que o presenteador participe (ou não) com o receptor no usufruto do item.

O entretenimento somente é apropriado quando usado para encorajar e promover relações de trabalho para a Gestora, observados, sempre os procedimentos e regras previstas neste Código.

A solicitação de Presentes e/ou Entretenimento é antiprofissional e estritamente proibida.

Os Colaboradores não deverão dar ou receber um Presente de qualquer pessoa com quem a Gestora teve ou tem relações de trabalho, exceto se previamente aprovado pelo Comitê de Compliance e Risco ou no caso de presentes, refeições, entretenimento ou outros benefícios com valor de até R$500,00 (quinhentos reais).

Os Colaboradores não deverão dar ou aceitar um convite que envolva Entretenimento o qual seja excessivo, não habitual ou incomum.

Caso os Colaboradores venham a receber Presentes e/ou Entretenimento de qualquer pessoa com quem a Gestora teve ou tem relações de trabalho, em valor superior ao limite estabelecido nesta Política, deverão reportar esta situação imediatamente a seu superior direto, o qual deverá informar o Diretor de Compliance, Risco e PLD e, caso o privilégio em questão represente algo desproporcional ao padrão, sendo passível de afetar sua independência, objetividade ou lealdade aos clientes da Gestora, o caso será analisado de maneira pontual pelo Comitê de Compliance e Risco.

No caso de entretenimento pessoal e/ou intransferível, o Colaborador deverá rejeitá-lo, exceto se previamente aprovado pelo Comitê de Compliance e Risco.

c) Soft Dollar

Os gestores de recursos devem transferir à carteira dos clientes qualquer benefício ou vantagem que possam alcançar em decorrência de sua condição de gestores da carteira.

Determinadas situações podem ter dinâmica diversa, como no caso das exceções previstas na regulamentação de fundos de investimento, ou no caso dos chamados "acordos de *Soft Dollar*".

Soft Dollar pode ser definido como sendo **(i)** o benefício econômico, de natureza não pecuniária, **(ii)** eventualmente concedido à Gestora por corretoras de títulos e valores mobiliários ou outros fornecedores ("Fornecedores"), **(iii)** em contraprestação ao direcionamento de transações das carteiras de valores mobiliários geridas pela Gestora, **(iv)** para fins de auxílio no processo de tomada de decisões de investimento.

Os exemplos mais comumente praticados pelo mercado para acordos de *Soft Dollar* estão relacionados aos serviços de análise de ativos e fornecimento de dados oferecidos por corretoras para auxílio na tomada de decisão de investimento pelos gestores de recursos.

Para que os acordos de *Soft Dollar* possam ser firmados, a Gestora deverá observar que os Fornecedores deverão ser considerados não somente em decorrência dos benefícios recebidos por meio de acordos de *Soft Dollar*, mas, primordialmente, em decorrência da eficiência, produtividade ou menores custos oferecidos por tais Fornecedores.

A Gestora, por meio de seus representantes, deverá observar os seguintes princípios ao firmar acordos de *Soft Dollar*:

(i) Colocar os interesses dos clientes acima de seus próprios interesses;

(ii) Definir de boa-fé se os valores pagos pelos clientes e, consequentemente, repassados aos Fornecedores, são razoáveis em relação aos serviços de execução de ordens ou outros benefícios que esteja recebendo;

(iii) Ter a certeza de que o benefício recebido auxiliará diretamente no processo de tomada de decisões de investimento em relação ao veículo que gerou tal benefício, devendo alocar os custos do serviço

recebido de acordo com seu uso, se o benefício apresentar natureza mista;

(iv) Divulgar amplamente a clientes, potenciais clientes e ao mercado os critérios e políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses oriundos da adoção de tais práticas; e

(v) Cumprir com seu dever de lealdade, transparência e fidúcia com os clientes.

Além disso, os acordos de *Soft Dollar*:

(i) Devem ser transparentes e sempre no melhor interesse dos clientes da Gestora;

(ii) Devem ser deve ser dada ciência ao time de Compliance, identificando, se possível, a capacidade de contribuírem diretamente para o processo de tomada de decisões de investimento, visando comprovar o racional que levou a firmar tais acordos de Soft Dollar*; e*

(iii) Não devem gerar qualquer vínculo de exclusividade ou de obrigação de execução de volume mínimo de transações os Fornecedores, devendo a Gestora manter a todo tempo total independência para selecionar e executar com quaisquer Fornecedores, sempre de acordo as melhores condições para seus clientes.

Ao contratar os serviços de execução de ordens, a Gestora não buscará somente o menor custo, mas o melhor custo-benefício, em linha com os critérios de *best execution* estabelecidos no mercado internacional, devendo ser capaz de justificar e comprovar que os valores pagos aos Fornecedores com os quais tenha acordos *Soft Dollar* são favoráveis aos fundos de investimento e carteiras sob sua gestão comparativamente a outras corretoras, considerados para tanto não apenas os custos aplicáveis, mas também a qualidade dos serviços oferecidos, que compreendem maior eficiência na execução de transações, condições de segurança, melhores plataformas de negociação, atendimento

diferenciado, provimento de serviço de análise de ações e qualidade técnica dos materiais correspondentes, disponibilização de sistemas de informação, entre outros.

Caso o benefício seja considerado de uso misto, os custos deverão ser alocados de forma razoável, de acordo com a utilização correspondente.

Benefícios não relacionados ao processo de tomada de decisão de investimentos não devem ser objeto de acordos de *Soft Dollar*.

4.6. 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) fomento de atividades de engajamento social dos Colaboradores.

Além disso, a Gestora incentiva seus Colaboradores a adotarem 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.

4.7. Política de Anticorrupção

a) <u>Introdução e Abrangência das Normas de Anticorrupção</u>

A Gestora está sujeita às normas e leis de anticorrupção, incluindo, mas não se limitando, às Normas de Anticorrupção, as quais 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).

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.

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.

b) 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) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

(ii) Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

(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) 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) 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.

c) 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.

d) Proibição de Doações Eleitorais

A Gestora não fará, doação a candidatos e/ou partidos políticos, uma vez que doações eleitorais por pessoas jurídicas são vedadas pela legislação eleitoral. Em relação às doações individuais dos Colaboradores, a Gestora e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

e) Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências ("Audiências") o Colaborador participante deverá, previamente ao encontro, avisar o Diretor de Compliance, Risco e PLD. Tal Colaborador sempre deverá 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.

4.8. Política de Certificação

a) Introdução

A Gestora aderiu e está sujeita às disposições do Código ANBIMA de Certificação, devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

b) Atividades Elegíveis e Critérios de Identificação.

Tendo em vista a atuação da Gestora, exclusivamente, como gestora de recursos de terceiros, a Gestora identificou, segundo o Código ANBIMA de Certificação, que a Certificação de Gestores ANBIMA ("CGA") é a única certificação descrita no Código ANBIMA de Certificação pertinente à sua atividade, sendo a CGA aplicável aos profissionais da Gestora com alçada/poder discricionário de investimento.

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.

Em complemento, a Gestora destaca que a CGA é certificação pessoal e intransferível. Caso o Colaborador esteja exercendo a atividade elegível de CGA 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 será de até 5 (cinco) anos. Por outro lado, caso o Colaborador não esteja exercendo a atividade elegível de CGA 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.

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.

c) Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a Área de Compliance e Risco 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, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, a Gestora deverá inserir o Colaborador no Banco de Dados da Gestora.

O Diretor de Investimentos deverá esclarecer à Área de Compliance e Risco se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de investimento.

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

A Área de Compliance e Risco 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.

A Área de Compliance e Risco deve incluir no Banco de Dados as informações cadastrais de todos os Colaboradores que tenham qualquer certificação ANBIMA, esteja a certificação vencida e/ou em processo de atualização.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer até o último dia do mês subsequente à data do evento que deu causa à atualização, nos termos do Art. 10, §1º, I das Regras e Procedimentos de Certificação da ANBIMA, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela Área de Compliance e Risco, sempre sob supervisão final do Diretor de Compliance, Risco e PLD, conforme disposto abaixo.

d) Rotinas de Verificação

Mensalmente, a Área de Compliance e Risco 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.

Ainda, o Diretor de Investimentos deverá contatar a Área de Compliance e Risco a fim de informá-los, prontamente, caso haja algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, além disso, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento.

Colaboradores que não possuam a CGA (ou a respectiva dispensa concedida pela ANBIMA, nos termos do Art. 11, III e §2º das Regras e Procedimentos de Certificação da ANBIMA e do documento "Orientações e Informações Técnicas para Certificações ANBIMA") 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, na qualidade de Profissional Titular, ou, em caso de sua indisponibilidade, do Profissional Suplente, ambos devidamente certificados e com poder discricionário de investimento, nos termos do Art. 20 das Regras e Procedimentos de Certificação da ANBIMA, tendo em vista que

tais colaboradores não possuem alçada/poder discricionário final de decisão para tanto, conforme Arts. 19 e 22 das mesmas Regras e Procedimentos.

Ademais, no curso das atividades de compliance e fiscalização desempenhadas pela Área de Compliance e Risco, 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 junto ao Comitê de Compliance e Risco, 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 ANBIMA 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 do departamento técnico envolvidos na atividade 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; e (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.

e) Processo de Afastamento

Todos os profissionais não certificados, em processo de certificação ou com a certificação vencida, e para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do Art. 8º, §1º, inciso V das Regras e Procedimentos de Certificação da ANBIMA, imediatamente afastados das Atividades Elegíveis aplicáveis até que obtenham ou atualizem a certificação, devendo o afastamento ser formalmente documentado pela Área de Compliance, observadas as exceções expressamente previstas nas Regras e Procedimentos de Certificação.

Os profissionais já certificados, caso deixem de ser Colaboradores da Gestora, deverão assinar a documentação prevista no **Anexo V** a este Manual denominado "Termo de Afastamento", comprovando o seu afastamento da Gestora. O mesmo procedimento de assinatura do **Anexo V** 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.

5. 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.

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 **TENAX CAPITAL 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.

São Paulo, [---] de [---] de [---].

_____

[**COLABORADOR**]

ANEXO II

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, doravante denominado Colaborador, e **TENAX CAPITAL LTDA,** inscrita no CNPJ sob o nº. [**43.777.696/0001-70**] ("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, 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 e carteiras geridas pela Gestora;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas 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 por prazo indeterminado após sua rescisão, 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 deste 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.

São Paulo, [---] de [---] de [---].

_____

[COLABORADOR]

_____

TENAX CAPITAL LTDA.

ANEXO III

PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DA TENAX CAPITAL LTDA.

1. Resolução CVM nº 50, de 31 de agosto de 2021;
2. Resolução CVM nº 175, de 23 de dezembro de 2022;
3. Resolução CVM 21/21;
4. Código de AGRT;
5. Regras e Procedimentos de Certificação ANBIMA;
6. Código de Ética;
7. Lei nº 12.846, de 1º de agosto de 2013;
8. Decreto nº 11.129, de 11 de julho de 2022; e
9. Lei 9.613/98, conforme alterada.

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 **TENAX CAPITAL 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.

São Paulo, [---] de [---] de [---].

_____

[COLABORADOR]

Apêndice
Lista dos Arquivos Gravados nos *Pen Drives*

ANEXO V

TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de alçada/poder final de decisão de investimentos e/ou desinvestimentos dos fundos sob gestão da **TENAX CAPITAL LTDA.** inscrita no CNPJ sob o nº. [**43.777.696/0001-70**] ("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. 16 do Código ANBIMA de Certificação, me conceda a isenção de obtenção da CGA; e

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

São Paulo, [---] de [---] de [---].

_____

[COLABORADOR]

_____

TENAX CAPITAL LTDA.

Testemunhas:

1._____ 2._____

Nome: Nome:

CPF: CPF: