POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS DA M&F CAPITAL LTDA.

Sumário

1. OBJETIVO

A presente Política de Compliance e Controles Internos ("**Política de Compliance e Controles Internos**") da M&F Capital Ltda. ("**M&F Capital**"), elaborada em conformidade a Resolução da Comissão de Valores Mobiliários ("**CVM**") nº 21 ("**Resolução CVM nº 21**"), de 25 de fevereiro de 2021, tem por objetivo estabelecer os procedimentos adotados internamente pela empresa, os quais, em conformidade com seus princípios e valores norteadores, determinam a aplicação das regras de conformidade de todos os aspectos inerentes às atividades da Gestora. A Política de Compliance e Controles Internos descrita nesse documento vincula todos os colaboradores da Gestora, incluindo sócios, administradores, empregados, contratados e estagiários da empresa, de forma que, qualquer um que preste serviços à Gestora, em qualquer posição, deve estar de acordo com as regras vigentes ("**Colaboradores**" ou "**Colaborador**").

Esta Política de Compliance e Controles Interno é parte integrante das regras que regem a relação societária e/ou de trabalho dos Colaboradores, sendo certo que os Colaboradores ao receberem a presente Política de Compliance e Controles Internos e demais Políticas da Gestora (conforme definido abaixo), deverão firmar Termo Recebimento e Compromisso, conforme previsto no Código de Ética e Conduta da Gestora.

A Política de Compliance e Controles Internos deverá ser revisada, no mínimo, anualmente, considerando, entre outros fatores, alterações na legislação e regulamentação aplicáveis, bem como eventuais deficiências identificadas em sua implementação. Adicionalmente, esta Política de Compliance e Controles Internos poderá ser atualizada a qualquer tempo, sempre que o Diretor de Compliance, Risco e PLD ou a Alta Administração (abaixo definidos) assim entenderem necessário, visando garantir sua efetividade e aderência ao perfil de risco da Gestora.

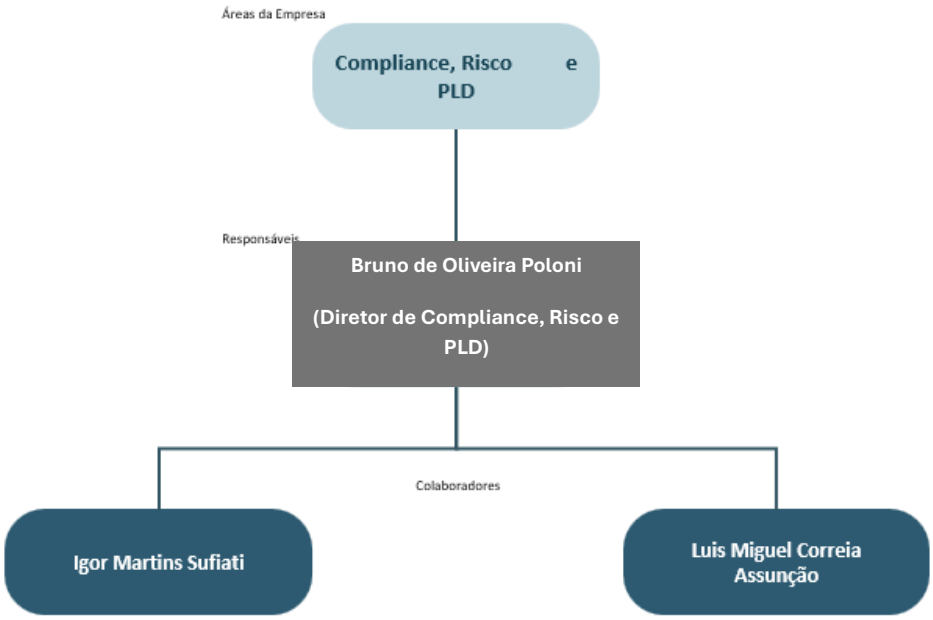
Além da Política de Compliance e Controles Internos, integram as políticas da Gestora, conforme disponibilizado em seu website ("**Políticas**"): (i) o Código de Ética e Conduta; (ii) a Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa ("**PLD/FTP**"); (iii) a Política de Gestão de Riscos; (iv) a Política de Rateio e Divisão de Ordens; (v) Política de Negociação de Valores Mobiliários; (vi) a Política de Suitability; (vii) a Política de Contratação de Terceiros; e (viii) a Política de Plano de Contingência. Eventuais termos iniciados em letras maiúsculas e não definidos nesta Política de Compliance e Controles Internos deverão ter o significado atribuído nas demais Políticas.

2. RESPONSABILIDADES DE OBRIGAÇÕES

2.1. Área de Compliance

A coordenação direta das atividades relacionadas a este Política de Compliance e Controles Internos é uma atribuição do Diretor de Compliance, Risco e PLD, diretor estatutário da Gestora, nos termos da Resolução CVM nº 21, conforme indicado no Formulário de Referência da Gestora. O Diretor de Compliance, Risco e PLD reporta-se somente à "**Alta Administração**" da Gestora, composta por seus diretores estatutários, sendo sua atuação pautada na autonomia e independência.

O Diretor de Compliance, Risco e PLD pode ser auxiliado por Colaboradores integrantes da "**Equipe de Compliance**", devidamente treinados, atualizados e com conhecimento compatível coma as respectivas funções desempenhadas ("**Área de Compliance**"). A Área de Compliance atua sob coordenação do Diretor de Compliance, Risco e PLD, exercendo suas atividades de forma completamente independente das outras áreas da Gestora.



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

(i) Acompanhar as regras descritas nesta Política de Compliance e Controles Internos;

(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 desta Política de Compliance e Controles Internos e das demais normas aplicáveis à atividade da Gestora para apreciação do Diretor de Compliance, Risco e PLD, ou, na sua ausência e/ou impedimento, da Alta Administração;

(iii) Atender prontamente todos os Colaboradores;

(iv) Identificar possíveis condutas contrárias a esta Política de Compliance e Controles Internos;

(v) Centralizar informações e revisões periódicas dos processos de compliance e controles internos, 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) Encaminhar à Alta Administração da Gestora, até o último dia útil do mês de abril de cada ano, relatório anual de compliance referente ao ano civil imediatamente anterior à data de entrega, nos termos do artigo 25 da Resolução CVM n° 21, contendo ("**Relatório de Compliance**"): (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, nos termos da Resolução CVM n° 21, conforme indicado no Formulário de Referência da Gestora ("**Diretor de Gestão**") 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;

(viii) Elaborar relatório anual listando as operações identificadas como suspeitas que tenham sido comunicadas às autoridades competentes, no âmbito da Política de PLD/FTP ("**Relatório de AIR**"), devendo referido relatório

permanecer disponível à CVM na sede da Gestora, sendo certo que este Relatório de AIR poderá constar no mesmo documento do Relatório de Compliance, mencionado acima;

(ix) Definir os princípios éticos a serem observados por todos os Colaboradores, constantes desta Política de Compliance e Controles Internos e das outras políticas internas da Gestora;

(x) Apreciar todos os casos que cheguem ao seu conhecimento sobre o potencial descumprimento dos preceitos éticos e de compliance previstos nesta Política de Compliance e Controles Internos ou nos demais documentos aqui mencionados, e apreciar e analisar situações não previstas;

(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 Diretor de Compliance, Risco e PLD;

(xiv) Analisar situações que cheguem ao seu conhecimento e que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais;

(xv) Promover a ampla divulgação e aplicação dos preceitos éticos no desenvolvimento das atividades de todos os Colaboradores, inclusive por meio da realização de treinamento inicial e treinamento periódico de reciclagem, podendo profissionais especializados serem contratados para conduzirem os treinamentos. Nesse sentido, deverá ser realizado um treinamento inicial, bem como de reciclagem anual de todos os seus Colaboradores, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem. Os treinamentos devem abordar: (i) as atividades da Gestora; (ii) os princípios éticos e de conduta da Gestora; (iii) as normas de compliance da Gestora previstas nesta Política de Compliance e Controles Internos; (iv) as demais Políticas e; (v) as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento das regras da Gestora.

2.2. Dúvidas e Denúncias

Esta Política de Compliance e Controles Internos 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, bem como eventual ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições desta Política de Compliance e Controles Internos e das demais normas aplicáveis às atividades da Gestora, deve ser dirigida pela pessoa aplicável ao Diretor de Compliance, Risco e PLD.

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos desta Política de Compliance e Controles Internos 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 esta Política de Compliance e Controles Internos. O Colaborador que se omitir de tal obrigação poderá sofrer as sanções definidas no item 2.4 desta Política de Compliance e Controles Internos.

Para promover denúncias e/ou comunicações sobre situações suspeitas, o Colaborador pode encaminhá-las, de forma anônima para os seguintes canais: ouvidoria@mfcapital.co e (16) 3877-6569. Caso a violação ou suspeita de violação recaia sobre o Diretor de Compliance, Risco e PLD, o Colaborador deverá informar diretamente a Alta Administração.

Todas as denúncias encaminhadas serão analisadas e, quando aplicável, investigadas e respondidas pelo Diretor de Compliance, Risco e PLD e/ou pela Alta Administração, conforme o caso.

É expressamente vedado qualquer tipo de ação vexatória ou retaliação contra o Colaborador que tenha realizado a denúncia, de forma que toda e qualquer denúncia será tratada com a máxima discrição e de forma confidencial.

2.3. Procedimentos

Mediante a ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nesta Política de Compliance e Controles Internos ou aplicáveis às atividades da Gestora, que cheguem ao conhecimento do Diretor de Compliance, Risco e PLD, de acordo com os procedimentos estabelecidos

nesta Política de Compliance e Controles Internos, este utilizará os registros e sistemas de monitoramento eletrônico referidos nesta Política de Compliance e Controles Internos para verificar a conduta dos Colaboradores envolvidos.

Nesse sentido, a Área de Compliance, sob coordenação e responsabilidade final do Diretor de Compliance, Risco e PLD:

(i) Poderá acessar, quando julgar oportuno e necessário, todo conteúdo que está na rede, inclusive arquivos pessoais salvos em cada computador utilizado como ferramenta de trabalho disponibilizado pela Gestora. Da mesma forma, mensagens de correio eletrônico de Colaboradores poderão ser gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que são ferramentas de trabalho disponibilizadas pela Gestora;

(ii) Escolherá aleatoriamente uma amostragem significativa dos Colaboradores e realizará um monitoramento, anualmente, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas na presente Política de Compliance e Controles Internos;

(iii) Verificará, 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; e

(iv) Analisará os controles previstos nesta Política de Compliance e Controles Internos, bem como em outras políticas da Gestora, propondo a criação de novos controles e melhorias naqueles que eventualmente sejam considerados deficientes, monitorando as respectivas correções, sendo que as análises e eventuais correções, se for o caso, deverão ser objeto do Relatório de Compliance.

O Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas nos monitoramentos descritos acima para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos desta Política de Compliance e Controles Internos e do Código de Ética e Conduta. 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.

2.4. Sanções

O Diretor de Compliance, Risco e PLD é responsável pela definição e aplicação das sanções aos Colaboradores que descumprirem as obrigações previstas nesta Política de Compliance e Controles Internos. Caso a conduta avaliada seja imputada ao próprio Diretor de Compliance, Risco e PLD, a definição e aplicação da sanção ficará a cargo da Alta Administração.

Em conformidade ao Código de Ética da Gestora, as sanções aplicáveis são: (i) advertência; (ii) suspensão; (iii) desligamento ou exclusão por justa causa; e (iv) demissão por justa causa.

3. INFORMAÇÕES E CONFIDENCIALIDADE

3.1. Sigilo e Conduta

Todos os Colaboradores deverão ler atentamente e entender o disposto nesta Política de Compliance e Controles Internos, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no "**Anexo I**" ("**Termo de Confidencialidade**").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial (conforme definido abaixo), 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 e de compliance da Gestora.

São consideradas informações confidenciais, reservadas ou privilegiadas ("**Informações Confidenciais**"), para os fins desta Política de Compliance e Controles Internos, 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, 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.

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 e/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.

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.

3.2. Insider Trading, Dicas e Front-Running

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem: (a) *Insider Trading*, ou seja, 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); (b) "Dica", ou seja, 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; e/ou (c) *Front-running*, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas aqui descritas 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 nesta Política de Compliance e Controles Internos e na legislação aplicável, incluindo eventual demissão por justa causa.

3.3. Divulgação de Fatos Relevantes

No âmbito da gestão de fundos de investimentos, em que pese seja responsabilidade do administrador fiduciário do fundo a operacionalização da divulgação de qualquer fato relevante ocorrido ou relacionado ao funcionamento do fundo, da classe ou aos ativos integrantes da carteira, assim que dele tiver conhecimento, é responsabilidade dos demais prestadores de serviços, incluindo a Gestora, informar imediatamente ao administrador fiduciário sobre os fatos relevantes de que venham a ter conhecimento, para a devida divulgação.

Nesse sentido, são considerados relevantes, nos termos do artigo 64, §1º da Parte Geral da Resolução CVM nº 175 ("**Resolução CVM nº 175**"), de 28 de dezembro de 2022,

quaisquer fatos que possam influir de modo ponderável no valor das cotas ou na decisão dos investidores de adquirir, resgatar, alienar ou manter cotas. São exemplos não exaustivos de fatos potencialmente relevantes:

(i) Alteração no tratamento tributário conferido ao fundo, à classe ou aos cotistas;

(ii) Contratação de formador de mercado e o término da prestação desse serviço;

(iii) Contratação de agência de classificação de risco, caso não estabelecida no regulamento do fundo ou no anexo da classe;

(iv) Mudança na classificação de risco atribuída ao fundo, à classe ou à subclasse de cotas;

(v) Alteração de prestador de serviço essencial;

(vi) Fusão, incorporação, cisão ou transformação do fundo ou da classe de cotas;

(vii) Alteração do mercado organizado em que seja admitida a negociação de cotas da classe do fundo;

(viii) Cancelamento da admissão das cotas do fundo ou da classe à negociação em mercado organizado; e

(ix) Emissão de cotas de fundo fechado.

Os fatos relevantes podem, de formar excepcional, não serem divulgados, caso seja entendido pela Gestora e pelo administrador fiduciário do fundo que sua revelação põe em risco interesse legítimo dos fundos ou de seus cotistas. Neste caso, tais informações serão tratadas como confidenciais até a Gestora e administrador fiduciário julgarem como oportuno o momento para sua divulgação.

Por outro lado, o administrador fiduciário fica obrigado a divulgar imediatamente fato relevante na hipótese de a informação escapar ao controle ou se ocorrer oscilação atípica na cotação, preço ou quantidade negociada de cotas, em havendo negociação em mercado regulado. A Gestora deverá notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

A Gestora deverá disponibilizar os fatos relevantes relativos aos fundos e classes sob

sua gestão em seu website.

3.4. Proteção de Dados Pessoais (LGPD)

A Gestora reconhece a importância da privacidade e da proteção dos dados pessoais tratados no âmbito de suas atividades, observando integralmente o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "**LGPD**") e nas demais normas aplicáveis.

No exercício de suas funções, todos os Colaboradores devem garantir que a coleta, o uso, o armazenamento, o compartilhamento e a eliminação de "**Dados Pessoais**" e "**Dados Sensíveis**", conforme definidos na LGPD, ocorram de forma segura, legítima e transparente, conforme as finalidades específicas da atividade desempenhada e os princípios previstos na LGPD.

A Gestora atua na qualidade de "**Controladora**" de Dados Pessoais, sendo responsável pelas decisões referentes ao tratamento de dados, e designará formalmente um Encarregado (DPO) para atuar como canal de comunicação entre os titulares, a Gestora e a Autoridade Nacional de Proteção de Dados (ANPD).

Os Colaboradores comprometem-se a observar as orientações e instruções fornecidas pela Gestora quanto ao tratamento adequado de dados pessoais, bem como a notificar imediatamente a Área de Compliance e o Encarregado sobre qualquer incidente, suspeita de violação ou acesso indevido a informações pessoais.

A violação das regras de proteção de dados sujeitará o infrator às sanções disciplinares internas previstas nesta Política Compliance e Controles Internos, sem prejuízo das responsabilidades civis, administrativas e criminais cabíveis.

4. SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Gestora e às disposições desta Política de Compliance e Controles Internos, 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 ter acesso restrito. Os computadores que serão utilizados pelos Colaboradores deverão estar 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 execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Área de Compliance, que será responsável, inclusive, por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito nesta Política de Compliance e Controles Internos.

4.1. Identificação de Riscos (*Risk Assessment*)

No âmbito de suas atividades, a Gestora identifica como principais riscos:

(i) **Dados e Informações**: 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;

(iv) **Governança da Gestão de Risco**: 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 Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("**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; e

(iv) **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 na identificação dos riscos 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.

4.2. Ações de Prevenção e Proteção

4.2.1. Regras Gerais 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.

Os arquivos físicos com os dados e informações relativos à atividade de administração de carteira de valores mobiliários e gestão de fundos de investimento desenvolvidos pela Gestora ficarão alocados na sede social da Gestora. 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.

O acesso a informações confidenciais e sigilosas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Gestora, a critério do Diretor de Compliance, Risco e PLD. O controle de acesso a tais

informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Diretor de Compliance, Risco e PLD, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa.

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 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 também mantém arquivo físico centralizado, porém, cada Colaborador é o responsável pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

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 devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pelo Diretor de Compliance, Risco e PLD.

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.

Downloads de qualquer natureza podem ser realizados, desde que de forma ponderada, respeitando o espaço individual de cada usuário. Periodicamente, a critério do Diretor de Compliance, Risco e PLD, poderão ser realizadas inspeções nos computadores para averiguação de *downloads* impróprios, não autorizados ou gravados em locais indevidos.

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. Neste caso, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora. As mensagens enviadas ou recebidas por meio de e-mails corporativos, seus respectivos anexos e a navegação por meio da rede mundial de computadores poderão ser monitoradas pela Gestora, a critério do Diretor de Compliance, Risco e PLD, a qualquer tempo e independentemente de prévia notificação ao Colaborador.

Os equipamentos e computadores disponibilizados aos Colaboradores deverão ser utilizados com a finalidade de atender aos interesses comerciais da Gestora, sendo permitida a sua utilização para fins particulares de forma moderada e que, de nenhuma forma, possa trazer riscos aos sistemas utilizados pela Gestora para realização de seus fins comerciais. 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.

4.2.2. Regras Específicas

Além das regras gerais de condutas, a Gestora adota as seguintes ações de proteção e prevenção em relação a segurança da informação e cibernética:

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 anualmente, 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 ao e-mail, rede e diretório, conforme requisição por estes e autorização pelo Diretor de Compliance, Risco e PLD. 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.
Controle de Acesso	O acesso de terceiros à Gestora somente é permitido na área de recepção. O acesso de pessoas estranhas à Gestora às áreas restritas somente é permitido com a autorização expressa do Diretor de Compliance, Risco e PLD. 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 um *hardware* de *firewall* projetado 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*). O sistema de prevenção a ataques será atualizado diariamente. 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 e por meio de *links* dedicados e seguros, via internet dedicada.

4.3. Monitoramento e Testes

A Área de Compliance 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, anual:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;

(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Gestora para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Gestora; e

(iii) 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.

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

4.4. 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	O Diretor de Compliance, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não

de Resposta 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); e

(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.

4.5. Arquivamento de Informações

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, bem como todos os documentos e informações exigidos pela Resolução CVM nº 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o art. 18, inciso IV, e art. 34, da Resolução CVM nº 21.

5. ANTICORRUPÇÃO

5.1. Introdução e Abrangência das Normas Anticorrupção

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 agentes 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 agentes públicos também devem ser considerados "agentes públicos" para os propósitos desta Política de Compliance e Controles Internos e das Normas de Anticorrupção.

Qualquer violação desta Política de Compliance e Controles Internos 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.

5.2. 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; e

(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.

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

5.4. 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.

5.5. 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, 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.

6. SEGREGAÇÃO DAS ATIVIDADES

Atualmente, a Gestora somente desempenha as atividades voltadas para a gestão de carteiras de títulos e valores mobiliários e distribuição de cotas das classes de fundos sob sua gestão, as quais são autorizadas e exercidas nos termos da Resolução CVM nº 21.

Segundo a CVM, para que tais atividades sejam devidamente exercidas de maneira regular, é necessário que estejam credenciadas e adequadas às regras aplicáveis para

sua categoria. Dentre essas regras, destaca-se que é obrigatório que haja a segregação entre as atividades de gestão de carteiras de títulos e valores mobiliários e de fundos de investimentos, de quaisquer outras atividades que a gestora venha a exercer, sejam elas exercidas pela própria gestora ou por prestadores de serviços ou terceirizados, com exceção da atividade de distribuição de cotas de classes de fundos de investimento prestada pela Gestora.

Neste sentido, caso a Gestora passe a exercer outra atividade regulada no mercado de capitais, assegurará aos Colaboradores, seus clientes e às autoridades reguladoras, a completa segregação de suas atividades, adotando procedimentos operacionais em prol da segregação física de instalações entre a Gestora e empresas responsáveis por diferentes atividades prestadas no mercado de capitais, bem como segregação sistemática e interna das atividades, garantindo que sejam exercidas sem quaisquer risco a outras atividades e vice versa.

Em relação às atividades de administração de carteiras de valores mobiliários e distribuição de cotas de classes de fundos sob sua gestão, a Gestora realiza segregação física e operacional entre a "**Área de Gestão**", sob responsabilidade do Diretor de Gestão, diretor estatutário da Gestora, nos termos da Resolução CVM nº 21, conforme indicado no Formulário de Referência da Gestora, e a "**Área de Distribuição**", sob responsabilidade do Diretor de Distribuição e Suitability, diretor estatutário da Gestora, nos termos da Resolução CVM nº 21, conforme indicado no Formulário de Referência da Gestora.

As atividades desenvolvidas pela Área de Gestão e pela Área de Distribuição são localizadas no mesmo imóvel, mas em salas separadas, de acesso restrito, sendo que o ingresso de terceiros só será permitido se autorizado pelo Diretor de Gestão ou pelo Diretor de Distribuição e Suitability, respectivamente, e desde que acompanhado de algum Colaborador da respectiva área.

A segregação virtual entre as áreas, que envolve a rede, sistemas e dados, é feita através do uso de controles de acesso entre as áreas de trabalho da Gestora. A liberação de acesso e o monitoramento destes são realizados pelo Diretor de Compliance, Risco e PLD. Apenas o Diretor de Compliance, Risco e PLD têm acesso à criação de usuários e à rede localizada nos servidores de dados e comunicação da Gestora. Cada Colaborador tem seu perfil de utilização, que é controlado pelo Diretor de Compliance, Risco e PLD. Além disso, usam-se redes de dados segregadas para os computadores dessas áreas.

7. 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 III à presente Política de Compliance e Controles Internos, 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.

8. PROGRAMAS DE TREINAMENTO

Para desempenho das atividades em consonância com as políticas e manuais vigente, a Área de Compliance irá promover o treinamento inicial de todos seus Colaboradores, especialmente aqueles que tenham acesso a Informações Confidenciais ou participem de processos de decisão de investimento, visando adquirir conhecimento sobre as atividades da Gestora e terá, ainda, a oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Além disso, todos os treinamentos abordarão as normas dispostas nas políticas e códigos aprovados pela Gestora relativas a cada um dos temas, apresentando aos Colaboradores seus principais aspectos e os mecanismos de execução, bem como as

penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras. Assim, deverão proporcionar aos Colaboradores uma visão geral das políticas adotadas pela Gestora, de forma que os Colaboradores se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

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.

Diariamente, a Gestora disponibilizará a todos os seus Colaboradores ferramentas eletrônicas de recebimento de informações financeiras, regulamentares, geopolíticas e estratégicas a nível global. Ademais, incentivará a participação de todos os seus Colaboradores em eventos pertinentes ao mercado financeiro e cursos específicos para determinadas necessidades.

A Gestora poderá, por deliberação da Alta Administração, financiar cursos de aprimoramento profissional, desde que julgue viável e interessante o conteúdo a ser lecionado. Caberá aos responsáveis pela área administrativa e financeira da Gestora a aprovação de participação em cursos, eventos ou palestras pelo Colaborador solicitante.

9. DIPOSIÇÕES GERAIS

Esta Política de Compliance e Controles Internos, aprovada pela Alta Administração da Gestora, encontra-se disponível para consulta (i) mediante solicitação direta à Área de Compliance da Gestora; ou (ii) por intermédio da rede mundial de computadores, via website: https://www.mfcapital.co/

Quaisquer dúvidas decorrentes desta Política de PLD/FTP poderão ser dirimidas pela Área de Compliance da Gestora, na Cidade de Ribeirão Preto, Estado de São Paulo, na Rua José Bianchi, nº 555, 22º Andar, Conj. 2214, "MF", Nova Ribeirânia, CEP 14.096-730, por meio do telefone (16) 99183-3410 ou, ainda, por meio do correio eletrônico: bruno.poloni@mfcapital.co.

10. HISTÓRICO DAS ATUALIZAÇÕES DA POLÍTICA DE COMPLIANCE E CONTROLES INTERNOS

Histórico das atualizações				
Data de Aprovação	**Versão**	**Aprovação**	**Responsável**	**Periodicidade de Revisão**

15 de abril de 2026	1ª	Alta Administração	Diretor de Compliance, Risco e PLD	Anual
14 de julho de 2026	2ª e atual	Alta Administração	Diretor de Compliance, Risco e PLD	Anual

ANEXO I

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, [--], inscrito no CPF/MF sob o nº [--], doravante denominado "**Colaborador**", e **M&F CAPITAL LTDA**., inscrita no CNPJ sob o nº. 57.187.567/0001-36 ("**M&F Capital**").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da M&F Capital, celebrar o presente Termo de Confidencialidade, 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 de Confidencialidade, 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 M&F Capital, seus sócios e clientes, aqui também contemplados os próprios fundos, 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, dos clubes, fundos de investimento e carteiras geridas pela M&F Capital;

(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela M&F Capital;

(iv) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da M&F Capital 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 M&F Capital e que ainda não foi devidamente levado à público;

(v) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;

(vi) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

(vii) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da M&F Capital 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 M&F Capital, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à M&F Capital, 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 de Confidencialidade 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 M&F Capital, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "Insider Trading", "Dicas" e "Front Running", seja atuando em benefício próprio, da M&F Capital ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo de Confidencialidade, 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 M&F Capital, 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 M&F Capital são e permanecerão sendo propriedade exclusiva da M&F Capital 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 M&F Capital, devendo todos os documentos permanecer em poder e sob a custódia da M&F Capital, salvo se em virtude de interesses da M&F Capital for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da M&F Capital;

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

(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 M&F Capital, 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 M&F Capital, permitindo que a M&F

Capital procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a M&F Capital 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 M&F Capital subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Tenho ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "**LGPD**") e me comprometo a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas em conformidade com o estabelecido pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela M&F Capital.

6.1. Estou ciente, ainda, de meu compromisso de comunicar ao Encarregado[1], conforme definido pela M&F Capital, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as orientações acerca da privacidade e do tratamento de informações fornecidas pela M&F Capital.

6.2. Na qualidade de pessoa física titular de Dados Pessoais ("**Titular de Dados Pessoais**"), estou ciente e de acordo que a M&F Capital, na qualidade de "**Controladora**" para fins de atendimento às disposições da LGPD, tome decisões relativas ao Tratamento de meus Dados Pessoais[2], incluindo operações como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração ("**Tratamento**") durante todo o período em que eles forem pertinentes, observados os princípios e as garantias ora estabelecidas pela referida lei.

6.3. Também na qualidade de Titular de Dados Pessoais, estou ciente de que, a qualquer tempo, mediante requisição à Controladora, tenho o direito de (i) confirmar

[1] "Encarregado" é a pessoa indicada pela Gestora para atuar como canal de comunicação entre os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados.

[2] Para os fins do presente Termo de Compromisso são considerados Dados Pessoais toda informação relacionada a uma pessoa física que a torne diretamente identificada ou identificável.

a existência de Tratamento e acessar meus Dados Pessoais, (ii) corrigir dados incompletos, inexatos ou desatualizados, (iii) solicitar a anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD, (iv) solicitar a portabilidade de meus Dados Pessoais a outro fornecedor de serviço, (v) solicitar a eliminação dos Dados Pessoais tratados com o meu consentimento, (vi) solicitar informações sobre o compartilhamento dos meus dados pela Controladora e sobre a possibilidade de não fornecer o consentimento e as consequências dessa negativa, e (vii) me opor ao Tratamento de meus Dados Pessoais em caso de descumprimento da LGPD.

6.4. Reconheço que a Controladora poderá compartilhar os Dados Pessoais com outros agentes de Tratamento de dados, tais como escritórios de contabilidade, agências de turismo, planos de saúde e instituições financeiras, caso seja necessário, bem como que poderá compartilhar em seu website os Dados Pessoais, incluindo minha identificação como Colaborador da M&F Capital e meu histórico profissional, observados os princípios e as garantias ora estabelecidos pela LGPD, com o que, desde já, estou de acordo.

6.5. Estou ciente de que a Controladora poderá manter armazenados os Dados Pessoais necessários após o término da relação contratual, por prazo determinado em lei, para fins de cumprimento de obrigações legais e/ou regulatórias, bem como para exercer seus direitos em processos administrativos e/ou judiciais.

6.6. Comprometo-me, enfim, a observar em tudo às instruções fornecidas pela M&F Capital, na qualidade de Controladora, acerca do Tratamento que deverá ser concedido aos Dados Pessoais aos quais tiver acesso em razão de minhas atividades, bem como a sempre agir de acordo com as disposições da LGPD e das normas internas da M&F Capital quanto à privacidade e proteção de Dados Pessoais.

7. Este Termo de Confidencialidade é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a M&F Capital, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

8. A transgressão a qualquer das regras descritas neste Termo de Confidencialidade, sem prejuízo do disposto no item 2.2 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da M&F Capital.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente Termo de Confidencialidade.

Ribeirão Preto/SP, [--] de [--] de [--].

_____

[COLABORADOR]

_____

M&F CAPITAL LTDA.

ANEXO II

TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, [--], inscrito no CPF/MF sob o nº [--], **DECLARO** para os devidos fins:

(i) que a disponibilização pelo Colaborador à **M&F CAPITAL LTDA**. ("**M&F Capital**"), nesta data, dos documentos contidos no pen drive da marca [--], número de série [--] ("**Documentos**"), bem como sua futura utilização pela M&F Capital, 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 M&F Capital, 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 M&F Capital, exceto se aprovado expressamente pela M&F Capital.

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

Os pen drives fazem parte integrante do presente Termo de Propriedade Intelectual, para todos os fins e efeitos de direito.

A lista de arquivos constantes dos pen drives se encontra no Apêndice ao presente Termo de Propriedade Intelectual.

Ribeirão Preto/SP, [--] de [--] de [--].

_____

[COLABORADOR]

Apêndice ao Termo de Propriedade Intelectual

Lista dos Arquivos Gravados nos Pen Drives

Nome	Formato	Última modificação
[--]	[--]	[--]
[--]	[--]	[--]
[--]	[--]	[--]
[--]	[--]	[--]