



## **MANUAL DE CONTROLES INTERNOS (*COMPLIANCE*)**

**JULHO / 2020**

## ÍNDICE

<b>1. INTRODUÇÃO E OBJETIVO</b> .....	<b>4</b>
<b>2. PROCEDIMENTOS</b> .....	<b>4</b>
2.1. <i>Designação de um Diretor Responsável</i> .....	4
2.2. <i>Revisão periódica e preparação de relatório</i> .....	6
2.3. <i>Treinamento</i> .....	6
2.4. <i>Apresentação do Manual de Compliance e suas modificações</i> .....	7
2.5. <i>Atividades Externas</i> .....	7
2.6. <i>Supervisão e responsabilidades</i> .....	7
2.7. <i>Sanções</i> .....	8
<b>3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO</b> ..	<b>8</b>
3.1. <i>Segurança da Informação Confidencial</i> .....	8
3.2. <i>Propriedade intelectual</i> .....	11
<b>4. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING</b> .....	<b>11</b>
4.1. <i>Insider Trading e “Dicas”</i> .....	12
<b>5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES</b> .....	<b>12</b>
5.1. <i>Segregação física</i> .....	12
5.2. <i>Segregação eletrônica</i> .....	13
5.3. <i>Segregação em relação às demais empresas nas quais os sócios e diretores da Pandhora tenham participação societária e/ou funcional</i> .....	14
5.4. <i>Especificidades dos mecanismos de controles internos</i> .....	14
<b>6. DIVULGAÇÃO DE MATERIAL DE MARKETING</b> .....	<b>15</b>
<b>7. APROVAÇÃO DE CORRETORAS E SOFT DOLLAR</b> .....	<b>18</b>
7.1. <i>Política de Soft Dollar</i> .....	18
<b>8. POLÍTICA DE KNOW YOUR CLIENT (KYC) E PREVENÇÃO À LAVAGEM DE DINHEIRO</b> .....	<b>19</b>
8.1. <i>Cadastro de clientes e atualização</i> .....	20
8.2. <i>Procedimentos relacionados às contrapartes</i> .....	23
8.3. <i>Pessoas politicamente expostas</i> .....	23
8.4. <i>Comunicações</i> .....	25
<b>9. ENVIO DE INFORMAÇÕES ÀS AUTORIDADES GOVERNAMENTAIS</b> .....	<b>27</b>
<b>10. PROCEDIMENTOS OPERACIONAIS</b> .....	<b>28</b>
10.1. <i>Registro de operações</i> .....	28
10.2. <i>Liquidação das Operações</i> .....	28

<b>11. PLANO DE CONTINUIDADE DO NEGÓCIO .....</b>	<b>28</b>
<b>12. SEGURANÇA CIBERNÉTICA .....</b>	<b>30</b>
<b>12.1. Avaliação dos riscos .....</b>	<b>30</b>
<b>12.2. Ações de prevenção e proteção.....</b>	<b>31</b>
<b>12.3. Plano de resposta.....</b>	<b>32</b>
<b>12.4. Reciclagem e revisão .....</b>	<b>33</b>
<b>ANEXO I - Modelo de Relatório Anual de <i>Compliance</i>.....</b>	<b>34</b>
<b>ANEXO II - Termo de Adesão .....</b>	<b>35</b>
<b>ANEXO III - Solicitação para Desempenho de Atividade Externa.....</b>	<b>37</b>

## 1. INTRODUÇÃO E OBJETIVO

O termo *Compliance* é originário do verbo, em inglês, *to comply*, e significa “estar em conformidade com regras, normas e procedimentos”.

Visto isso, a **PANDHORA INVESTIMENTOS LTDA.** (“Gestora”) adotou em sua estrutura as atividades de “Controles Internos” ou “*Compliance*”. O diretor responsável pelo *Compliance* (“Diretor de Compliance”) tem como objetivo garantir o cumprimento das leis e regulamentos emanados de autoridades competentes aplicáveis às atividades de Gestora, bem como as políticas e manuais da Gestora, e obrigações de fidúcia e lealdade devidas aos fundos de investimento e demais clientes cujas carteiras de títulos e valores mobiliários sejam geridas pela Gestora (“Clientes”), prevenindo a ocorrência de violações, detectando as violações que ocorram e punindo ou corrigindo quaisquer de tais descumprimentos.

Este Manual de Controles Internos (*Compliance*) (“Manual de Compliance”) foi elaborado para atender especificamente às atividades desempenhadas pela Gestora, de acordo com natureza, complexidade e riscos a elas inerentes, observada a obrigação de revisão e atualização periódica nos termos do item 2 abaixo.

Este Manual de *Compliance* é aplicável a todos os sócios, diretores, funcionários, empregados, estagiários e demais colaboradores da Gestora (em conjunto os “Colaboradores” e, individualmente e indistintamente, o “Colaborador”).

Este Manual de *Compliance* deve ser lido em conjunto com o Código de Ética da Gestora, que também contém regras que visam a atender aos objetivos aqui descritos.

Este Manual de *Compliance* está de acordo com o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como com a regulamentação vigente emitida pela Comissão de Valores Mobiliários (“CVM”).

## 2. PROCEDIMENTOS

### 2.1. *Designação de um Diretor Responsável*

A área de *Compliance* da gestora é liderada pelo Diretor de *Compliance*, Sr. Leandro Alves da Silva, devidamente nomeado no contrato social da Gestora.

O Diretor de *Compliance* exerce suas funções com plena independência e não atua em funções que possam afetar sua isenção, dentro ou fora da Gestora. Da mesma forma, a

área de *Compliance* não está sujeita a qualquer ingerência por parte da equipe de gestão e possui autonomia para questionar os riscos assumidos nas operações realizadas pela Gestora.

O Diretor de *Compliance* é o responsável pela implementação geral dos procedimentos previstos neste Manual de *Compliance*, e caso tenha que se ausentar por um longo período, deverá ser substituído ou deverá designar um responsável temporário para cumprir suas funções durante este período de ausência. Caso esta designação não seja realizada, caberá aos sócios da Gestora fazê-lo.

O Diretor de *Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Gestora no que concerne a esclarecimentos de todos os controles e regulamentos internos (*Compliance*), bem como no acompanhamento de conformidade das operações e atividades da Gestora com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

São também atribuições do Diretor de *Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

- (i) Implantar o conceito de controles internos através de uma cultura de *Compliance*, visando melhoria nos controles;
- (ii) Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;
- (iii) Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no “Código de Ética”, assim como avaliar as demais situações que não foram previstas em todas as políticas internas da Gestora (“Políticas Internas”);
- (iv) Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;
- (v) Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;
- (vi) Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

- (vii) Reconhecer situações novas no cotidiano da administração interna ou nos negócios da Gestora que não foram planejadas, fazendo a análise de tais situações;
- (viii) Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Gestora;
- (ix) Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Gestora, assim como das pessoas envolvidas no caso.

## **2.2. *Revisão periódica e preparação de relatório***

O Diretor de *Compliance* deverá revisar pelo menos anualmente este Manual de *Compliance* para verificar a adequação das políticas e procedimentos aqui previstos, e sua efetividade. Tais revisões periódicas deverão levar em consideração, entre outros fatores, as violações ocorridas no período anterior, e quaisquer outras atualizações decorrentes da mudança nas atividades realizadas pela Gestora.

O Diretor de *Compliance* deve encaminhar aos diretores da Gestora, até o último dia do mês de janeiro de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) a manifestação a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las, que deverá seguir o formato previsto no Anexo I.

O relatório referido no parágrafo acima deverá ficar disponível para a CVM na sede da Gestora.

## **2.3. *Treinamento***

A Gestora possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre as Políticas Internas, inclusive este Manual de *Compliance*, aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento.

A equipe de *Compliance* deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser recomendável, de forma que os Colaboradores entendam e cumpram as disposições previstas neste manual, e deve estar frequentemente

disponível para responder questões que possam surgir em relação aos termos deste Manual de *Compliance* e quaisquer regras relacionadas a *Compliance*.

A periodicidade mínima do processo de reciclagem continuada será anual. A cada processo de reciclagem continuada, os Colaboradores assinarão termo comprovando a participação no respectivo processo.

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

#### **2.4. Apresentação do Manual de Compliance e suas modificações**

O Diretor de *Compliance* deverá entregar uma cópia deste Manual de *Compliance*, e das Políticas Internas, para todos os Colaboradores por ocasião do início das atividades destes na Gestora, e sempre que estes documentos forem modificados. Mediante o recebimento deste Manual de *Compliance*, o Colaborador deverá confirmar que leu, entendeu e cumpre com os termos deste Manual de *Compliance* e das Políticas Internas, mediante assinatura do termo de adesão que deverá seguir o formato previsto no Anexo II (“Termo de Adesão”).

#### **2.5. Atividades Externas**

Os Colaboradores devem obter a aprovação escrita do Diretor de *Compliance* antes de envolverem-se em negócios externos à Gestora. “Atividades Externas” incluem ser um diretor, conselheiro ou sócio de sociedade ou funcionário ou consultor de qualquer entidade ou organização (seja em nome da Gestora ou não). Os Colaboradores que desejam ingressar ou engajar-se em tais Atividades Externas devem obter a aprovação prévia por escrito do Diretor de *Compliance* por meio da “Solicitação para Desempenho de Atividade Externa” na forma do Anexo III.

Não será necessária a prévia autorização do Diretor de *Compliance* para Atividades Externas relacionadas à caridade, organizações sem fins lucrativos, clubes ou associações civis.

#### **2.6. Supervisão e responsabilidades**

Todas as matérias de violações a obrigações de *Compliance*, ou dúvidas a elas relativas, que venham a ser de conhecimento de qualquer Colaborador devem ser prontamente informadas ao Diretor de *Compliance*, que deverá investigar quaisquer possíveis violações de regras ou procedimentos de *Compliance*, e determinar quais as sanções

aplicáveis. O Diretor de *Compliance* poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

## **2.7. Sanções**

As sanções decorrentes do descumprimento das regras estabelecidas neste Manual de *Compliance* e/ou das Políticas Internas serão definidas e aplicadas pelo Diretor de *Compliance*, a seu critério razoável, garantido ao Colaborador, contudo, amplo direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, se aplicável, nos termos da legislação vigente, sem prejuízo da aplicação de penalidades pela CVM e do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio dos procedimentos legais cabíveis.

## **3. POLÍTICA DE CONFIDENCIALIDADE E TRATAMENTO DA INFORMAÇÃO**

Nos termos da Instrução CVM nº 558, de 26 de março de 2015, especialmente o Artigo 24, III e Artigo 25, II, a Gestora adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Gestora é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

### **3.1. Segurança da Informação Confidencial**

A Gestora mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, diretórios de rede, planos de continuidade entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da Gestora, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento da Gestora, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna da Gestora.



Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e Clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de *Compliance*.

Todos os Colaboradores, assim como todos os terceiros contratados pela Gestora, deverão assinar documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais.

É terminantemente proibido que os Colaboradores façam cópias 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 informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora e de seus Clientes. 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.

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

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, 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 pela área de *Compliance*.

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

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

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

A equipe de *Compliance* também monitorará e será avisada por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Diretor de *Compliance* elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via *internet (downloads)*, sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador.

Todas as informações do servidor da Gestora, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área, sendo armazenadas com *backup*.

Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de *Compliance* apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Gestora, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

### **3.2. Propriedade intelectual**

Todos os documentos desenvolvidos na realização das atividades da Gestora ou a elas diretamente relacionados, tais quais, sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise etc., são de propriedade intelectual da Gestora.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual da Gestora fora do escopo de atuação ou não destinado aos Clientes, dependerá de prévia e expressa autorização por escrito do Diretor de *Compliance*.

Uma vez rompido com a Gestora o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

## **4. INFORMAÇÃO PRIVILEGIADA E INSIDER TRADING**

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um Cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Gestora que possa influir de modo ponderável: (a) na rentabilidade dos valores mobiliários administrados pela Gestora; (b) na decisão de Clientes de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e (c) na decisão dos Clientes de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso de o Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de *Compliance*, não podendo comunicá-la a

ninguém, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao Diretor de *Compliance*.

#### **4.1. *Insider Trading e “Dicas”***

*Insider trading* baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo a própria Gestora e seus Colaboradores).

“Dica” é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

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

A prática de qualquer ato em violação deste Manual de *Compliance* pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, deste Manual de *Compliance*, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Instrução CVM nº 358, de 03 de janeiro de 2002 (“Instrução CVM 358”).

É de responsabilidade do Diretor de *Compliance* verificar e processar periodicamente as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e “dicas”. Casos envolvendo o uso de informação privilegiada, *insider trading* e “dicas” devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com a Gestora, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

## **5. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES**

### **5.1. *Segregação física***

Caso a Gestora venha a desenvolver atividades que apresentem conflito de interesses com a atividade de gestão, a área de gestão de recursos da Gestora será fisicamente segregada das demais, sendo o acesso restrito aos Colaboradores integrantes da área, por meio de controle de acesso nas portas, para garantir que não exista circulação de informações que possam gerar conflito de interesses (“*chinese wall*”).

Não será permitida a circulação de Colaboradores em seções que não sejam destinadas ao respectivo Colaborador.

Reuniões com terceiros não Colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não Colaborador, inclusive Clientes, sendo este encaminhado diretamente à devida sala.

É de competência do Diretor de *Compliance*, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções. Caso o Diretor de *Compliance* constate que o Colaborador tenha tentado acesso às áreas restritas com frequência acima do comum ou necessária, ou ainda sem qualquer motivo aparente, poderá aplicar as devidas sanções. Eventual infração à regra estabelecida neste Manual de *Compliance* será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Diretor de *Compliance*.

A propósito, as tarefas contábeis da empresa são terceirizadas, de modo que são exercidas no local de atuação das empresas contratadas (RN Contadores Associados).

## **5.2. Segregação eletrônica**

Adicionalmente, a Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado, sendo certo que tal restrição/segregação será feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Ademais, cada Colaborador terá acesso apenas às pastas de arquivos internos às quais o Diretor de *Compliance* e a área de TI tenha lhe concedido a permissão de acesso, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Gestora permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

### **5.3. *Segregação em relação às demais empresas nas quais os sócios e diretores da Pandhora tenham participação societária e/ou funcional***

Os sócios e diretores da Pandhora possuem participações e/ou atividades de representação em outros negócios, incluindo empresas de participações (holdings) e empresas prestadoras de serviços não financeiros (tais como consultoria, desenvolvimento de softwares etc) e financeiros (gestoras de recursos e agentes autônomos de investimentos). Nesse sentido, com o intuito de segregar a atividade de gestão de recursos e evitar qualquer compartilhamento de informação, a Gestora determina que os sócios que possuam participação societária e/ou funcional em outras empresas atuantes no mercado financeiro e de capitais não poderão ter atuação funcional na Pandhora, figurando apenas como sócios de capital, exceto se tais empresas atuem em nichos de mercados distintos daquele onde a Pandhora atua (como private equity/venture capital, direitos creditórios etc), de modo a não gerar conflito de interesses entre ambas as funções.

### **5.4. *Especificidades dos mecanismos de controles internos***

A Gestora, por meio do Diretor de *Compliance*, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

- (i) Definição de responsabilidades dentro da Gestora;
- (ii) Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;

- (iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;
- (iv) Contínua avaliação dos diversos riscos associados às atividades da empresa; e
- (v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Gestora estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de *Compliance*.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e *softwares* sobre os quais a Gestora possua licença de uso, acesso à *internet*, bem como materiais e suporte necessário, com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da Gestora. A esse respeito, o Diretor de *Compliance* poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro da Gestora.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Gestora, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual de *Compliance*, especialmente as informações mantidas em meio eletrônico.

## **6. DIVULGAÇÃO DE MATERIAL DE *MARKETING***

Todos os Colaboradores devem ter ciência de que a divulgação de materiais de *marketing* deve ser realizada estritamente de acordo com as regras emitidas pela CVM e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, e que não devem conter qualquer informação falsa ou que possa levar o público a erro.

Materiais de *marketing* devem ser entendidos como qualquer nota, circular, carta ou outro tipo de comunicação escrita, destinada a pessoas externas à Gestora, ou qualquer nota ou anúncio em qualquer publicação, rádio ou televisão, que ofereça qualquer serviço de



consultoria ou gestão prestado pela gestora, ou um produto de investimento da Gestora no mercado de valores mobiliários (incluindo fundos geridos).

Quaisquer materiais de *marketing* devem ser previamente submetidos à equipe de *Compliance*, que deverá verificar se está ou não de acordo com as várias regras aplicáveis, incluindo sem limitação a Instrução CVM nº 400, de 29 de dezembro de 2003 (“Instrução CVM 400”), a Instrução CVM nº 476, de 16 de janeiro de 2009 (“Instrução CVM 476”), a Instrução CVM nº 555, de 17 de dezembro de 2014 (“Instrução CVM 555”), o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, e diretrizes escritas emanadas da ANBIMA. O Diretor de *Compliance* deverá, quando necessário, valer-se de assessores externos para verificar o cumprimento das referidas normas. Somente após a aprovação por escrito do Diretor de *Compliance* é que qualquer material de *marketing* deve ser utilizado.

Abaixo encontra-se uma lista não exaustiva de regras aplicáveis a materiais de *marketing* de fundos de investimento.

Nos termos da Instrução CVM 555, qualquer material de divulgação do fundo deve, observadas as exceções previstas nas regras aplicáveis:

- (i) ser consistente com o regulamento e com a lâmina, se houver;
- (ii) ser elaborado em linguagem serena e moderada, advertindo seus leitores para os riscos do investimento;
- (iii) ser identificado como material de divulgação;
- (iv) mencionar a existência da lâmina, se houver, e do regulamento, bem como os endereços na rede mundial de computadores nos quais tais documentos podem ser obtidos;
- (v) ser apresentado em conjunto com a lâmina, se houver;
- (vi) conter as informações do item 12 do Anexo 42 da Instrução CVM 555, se a divulgação da lâmina não for obrigatória;
- (vii) conter informações: (a) verdadeiras, completas, consistentes e não induzir o Cliente a erro; (b) escritas em linguagem simples, clara, objetiva e concisa; e (c) úteis à avaliação do investimento; e (d) que não assegurem ou sugiram a existência de garantia de resultados futuros ou não isenção de risco para o Cliente.



Informações factuais devem vir acompanhadas da indicação de suas fontes e ser diferenciadas de interpretações, opiniões, projeções e estimativas.

Qualquer divulgação de informação sobre os resultados de fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses, a partir da data da primeira emissão de cotas.

Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente:

- (i) mencionar a data do início de seu funcionamento;
- (ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e a rentabilidade acumulada nos últimos 12 (doze) meses, não sendo obrigatória, neste caso, a discriminação mês a mês, ou no período decorrido desde a sua constituição, se inferior, observado que a divulgação de rentabilidade deve ser acompanhada de comparação, no mesmo período, com índice de mercado compatível com a política de investimento do fundo, se houver;
- (iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde a sua constituição, se mais recente;
- (iv) divulgar a taxa de administração e a taxa de performance, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e
- (v) destacar o público alvo do fundo e as restrições quanto à captação, de forma a ressaltar eventual impossibilidade, permanente ou temporária, de acesso ao fundo por parte de investidores em geral.

Caso o administrador contrate os serviços de empresa de classificação de risco, deve apresentar, em todo o material de divulgação, o grau mais recente conferido ao fundo, bem como a indicação de como obter maiores informações sobre a avaliação efetuada.

Ficam incorporadas por referência, ainda, as disposições do Capítulo VI do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como das “Diretrizes para Publicidade e Divulgação de Material Técnico de Fundos de Investimento” da ANBIMA, disponíveis publicamente no *website* desta instituição.

## 7. APROVAÇÃO DE CORRETORAS E *SOFT DOLLAR*

A equipe de *Compliance* manterá uma lista de corretoras aprovadas com base nos critérios estabelecidos pela Gestora. O *trader* executará ordens exclusivamente com corretoras constantes referida lista, exceto se receber a autorização prévia do Diretor de *Compliance* para usar outra corretora. O Diretor de *Compliance* atualizará a lista de corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

Os custos de transação mais relevantes tais como corretagem, emolumentos e custódia, devem ser constantemente monitorados, com o objetivo de serem minimizados. Semestralmente, o time de gestão da Gestora deve elaborar um *ranking* com critérios objetivos de corretoras levando em consideração qualidade do serviço e preço, visando encontrar a melhor equação e prezando o dever fiduciário que temos para com os nossos Investidores. A Gestora somente utilizará as corretoras mais bem classificadas.

As equipes de gestão e de *Compliance* devem rever o desempenho de cada corretora e considerar, entre outros aspectos: a qualidade das execuções fornecidas; o custo das execuções, acordos de *soft dollar* e potenciais conflitos de interesse.

### 7.1. *Política de Soft Dollar*

Quaisquer acordos envolvendo *soft dollars* devem ser previamente aprovados pelo Diretor de *Compliance*. *Soft dollars* podem ser definidos como quaisquer benefícios oferecidos por uma corretora a uma gestora que direcione ordens para a corretora, que podem incluir, sem limitação, *researches* e acesso a sistemas de informações de mercado como o *Bloomberg*.

Acordos de *soft dollar* somente poderão ser aceitos pelo Diretor de *Compliance* se quaisquer benefícios oferecidos (i) possam ser utilizados diretamente para melhorias da tomada de decisão de investimento pela Gestora; (ii) sejam razoáveis em relação ao valor das comissões pagas; e (iii) não afetem a independência da Gestora.

A prática de *soft dollar* é aceita única e exclusivamente para as atividades diretamente relacionadas à gestão dos recursos dos Clientes.

Os acordos de *soft dollars* não criam nenhuma obrigação para a Gestora operar exclusivamente junto às corretoras que concedem os benefícios.

## 8. POLÍTICA DE *KNOW YOUR CLIENT* (KYC) E PREVENÇÃO À LAVAGEM DE DINHEIRO

O termo “lavagem de dinheiro” abrange diversas atividades e processos com o propósito de ocultar o proprietário e a origem precedente de atividade ilegal, para simular uma origem legítima. A Gestora e seus Colaboradores devem obedecer todas as regras de prevenção à lavagem de dinheiro, aplicáveis às atividades de gestão de fundos de investimento, em especial a Lei nº 9.613, de 03 de março de 1998, conforme alterada (“Lei 9.613/98”), e a Instrução CVM nº 301, de 16 de abril de 1999 (“Instrução CVM 301”), cujos principais termos estão refletidos neste Manual de *Compliance*.

O Diretor de *Compliance* será responsável perante a CVM pelo cumprimento de todas as normas e regulamentação vigentes relacionados ao combate e à prevenção à lavagem de dinheiro.

O Diretor de *Compliance* estabelecerá o devido treinamento dos Colaboradores da Gestora – na forma deste Manual de *Compliance* – para que estes estejam aptos a reconhecer e a combater a lavagem de dinheiro, bem como providenciará novos treinamentos, se necessários, no caso de mudanças na legislação aplicável.

A Gestora adota os seguintes procedimentos permanentes de controle e vigilância, visando minimizar o risco de ocorrência de lavagem de dinheiro nas diversas operações financeiras sob sua responsabilidade, a saber:

- (i) Análise, pela equipe de *Compliance*, das movimentações financeiras que possam indicar a existência de crime, em razão de suas características, valores, formas de realização e instrumentos utilizados, ou que não apresentem fundamento econômico ou legal;
- (ii) Evitar realizar qualquer operação comercial ou financeira por conta de terceiros, a não ser que seja transparente, justificada e sólida, além de viabilizada ou executada através de canais bancários;
- (iii) Evitar operações com pessoas ou entidades que não possam comprovar a origem do dinheiro envolvido;
- (iv) Evitar operações financeiras internacionais complexas, que envolvam muitas movimentações de dinheiro em países diferentes e/ou entre bancos diferentes;
- (v) Avaliação das políticas e práticas de prevenção e combate à lavagem de dinheiro adotada por terceiros/parceiros da Gestora;

- (vi) Verificação da adequação ao perfil da Gestora dos Clientes oriundos dos distribuidores de cotas de fundos de investimento cujas carteiras sejam geridas pela Gestora;
- (vii) Registro e guarda das informações relativas às operações e serviços financeiros dos Clientes;
- (viii) Comunicação ao Conselho de Controle de Atividades Financeiras (“COAF”) e à CVM, no prazo legal, de propostas e/ou operações consideradas suspeitas ou atípicas, a menos que não seja objetivamente permitido fazê-lo;
- (ix) Comunicação ao COAF e à CVM de operações em espécie, ou cujo montante atinja os patamares fixados pelos reguladores;
- (x) Revisão periódica dos procedimentos e controles de prevenção e combate à lavagem de dinheiro e de controles internos;
- (xi) Adoção de procedimento de especial atenção a PPE, conforme definido abaixo; e
- (xii) Ter adequado conhecimento dos Colaboradores e fazê-los conhecer políticas e normativos aderentes aos órgãos reguladores.

A Gestora adota procedimentos que permitem o monitoramento das faixas de preços das cotas de fundos geridos distribuídas, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas, e se for o caso, comunicados aos órgãos competentes.

### **8.1. Cadastro de clientes e atualização**

Nos termos da Instrução CVM 301, o cadastro dos Clientes da Gestora deve abranger, no mínimo, as informações e documentos indicados abaixo:

- (i) Pessoa física: (a) nome completo, sexo, profissão, data de nascimento, naturalidade, nacionalidade, estado civil, filiação, nome do cônjuge ou companheiro; (b) natureza e número do documento de identificação, nome do órgão expedidor e data de expedição; (c) número de inscrição no Cadastro de Pessoas Físicas (“CPF/MF”); (d) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP) e número de telefone; (e) endereço eletrônico para correspondência; (f) ocupação profissional e entidade para a qual trabalha; (g) informações sobre os rendimentos e a situação patrimonial; (h) informações sobre perfil de risco e conhecimento financeiro do Cliente; (i) se o Cliente autoriza ou não a transmissão de ordem por procurador; (j) a indicação de

se há procuradores ou não; (k) qualificação dos procuradores e descrição de seus poderes, se houver; (l) datas das atualizações do cadastro; (m) assinatura do Cliente; (n) cópia dos seguintes documentos: documento de identidade e comprovante de residência ou domicílio; e (o) cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.

- (ii) Pessoa jurídica: (a) a denominação ou razão social; (b) nomes e CPF/MF dos controladores diretos ou razão social e inscrição no Cadastro Nacional de Pessoa Jurídica (“CNPJ”) dos controladores diretos; (c) nomes e CPF/MF dos administradores; (d) nomes dos procuradores; (e) número de CNPJ e NIRE; (f) endereço completo (logradouro, complemento, bairro, cidade, unidade da federação e CEP); (g) número de telefone; (h) endereço eletrônico para correspondência; (i) atividade principal desenvolvida; (j) faturamento médio mensal dos últimos doze meses e a situação patrimonial; (k) informações sobre perfil de risco e conhecimento financeiro do Cliente; (l) denominação ou razão social de pessoas jurídicas controladoras, controladas ou coligadas; (m) se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas; (n) se o Cliente autoriza ou não a transmissão de ordens por representante ou procurador; (o) qualificação dos representantes ou procuradores e descrição de seus poderes; (p) datas das atualizações do cadastro; (q) assinatura do Cliente; (r) cópia dos seguintes documentos: CNPJ, documento de constituição da pessoa jurídica devidamente atualizado e registrado no órgão competente, e atos societários que indiquem os administradores da pessoa jurídica, se for o caso; e (s) cópias dos seguintes documentos, se for o caso: procuração e documento de identidade do procurador.
- (iii) Demais hipóteses: (a) a identificação completa dos Clientes; (b) a identificação completa de seus representantes e/ou administradores; (c) situação financeira e patrimonial; (d) informações sobre perfil de risco e conhecimento financeiro do Cliente; (e) se o Cliente opera por conta de terceiros, no caso dos administradores de fundos de investimento e de carteiras administradas; (f) datas das atualizações do cadastro; e (g) assinatura do Cliente.

Em caso de Clientes não residentes no país, o cadastro deve, adicionalmente, conter: (i) os nomes das pessoas naturais autorizadas a emitir ordens e, conforme o caso, dos administradores da instituição ou responsáveis pela administração da carteira; e (ii) os nomes do representante legal e do responsável pela custódia dos seus valores mobiliários. Ainda, a Gestora adotará procedimentos para identificação da pessoa natural caracterizada como beneficiário final, nos termos da legislação e regulamentação vigentes.

As alterações ao endereço constante do cadastro dependem de ordem do Cliente, escrita ou por meio eletrônico, e comprovante do correspondente endereço.

Do cadastro deve constar declaração, datada e assinada pelo Cliente ou, se for o caso, por procurador legalmente constituído, de que (conforme aplicável):

- (i) são verdadeiras as informações fornecidas para o preenchimento do cadastro;
- (ii) o Cliente se compromete a informar, no prazo de 10 (dez) dias, quaisquer alterações que vierem a ocorrer nos seus dados cadastrais, inclusive eventual revogação de mandato, caso exista procurador;
- (iii) o Cliente é pessoa vinculada ao intermediário, se for o caso;
- (iv) o Cliente não está impedido de operar no mercado de valores mobiliários;
- (v) suas ordens devem ser transmitidas por escrito, por sistemas eletrônicos de conexões automatizadas ou telefone e outros sistemas de transmissão de voz; e
- (vi) o Cliente autoriza os intermediários, caso existam débitos pendentes em seu nome, a liquidar os contratos, direitos e ativos adquiridos por sua conta e ordem, bem como a executar bens e direitos dados em garantia de suas operações ou que estejam em poder do intermediário, aplicando o produto da venda no pagamento dos débitos pendentes, independentemente de notificação judicial ou extrajudicial.

A critério exclusivo da Gestora, nos casos em que entender necessário, poderão ser requeridas, adicionalmente à documentação e informações previstas acima, visitas *due diligence* na residência, local de trabalho ou instalações comerciais do Cliente.

Após a análise e verificação, pela equipe de *Compliance*, dos documentos e informações fornecidos pelo Cliente, o Diretor de *Compliance* decidirá pela aprovação ou recusa do cadastro do Cliente. O fornecimento da totalidade dos documentos e informações solicitados não é garantia da aprovação do cadastro do Cliente, podendo a Gestora recusar o cadastramento de Clientes a seu exclusivo critério.

O cadastro de cada cliente ativo (assim entendido aquele que tenha efetuado movimentações ou apresente saldo no período de 24 (vinte e quatro) meses posteriores à última atualização), deve ser atualizado em intervalos não superiores a 24 (vinte e quatro) meses.

O processo de atualização deve ser evidenciado por meio de fichas cadastrais e/ou cartas assinadas pelos Clientes, *logs* de sistemas, gravações telefônicas, entre outros comprovantes de confirmação de dados. Nenhuma operação deve ser realizada para a carteira de Clientes cujo cadastro esteja incompleto.

Quaisquer dúvidas relativas a cadastro e suas atualizações devem ser submetidas à equipe de *Compliance*.

## **8.2. Procedimentos relacionados às contrapartes**

A Gestora é responsável por tomar todas as medidas necessárias, segundo a legislação e regulamentação aplicável, incluindo, mas não limitado a, Lei 9.613/98, Instrução CVM 301 e Ofício-Circular nº 5/2015/SIN/CVM, as regras de KYC (“conheça seu cliente”) presentes neste Manual de *Compliance* e as melhores práticas adotadas pelas entidades autorreguladoras do mercado, para estabelecer e documentar a verdadeira e completa identidade, situação financeira e o histórico de cada contraparte nas operações realizadas pelos fundos de investimento.

Nesse sentido, além dos clientes de suas carteiras, a Gestora busca analisar e monitorar, para fins de cumprimento às normas de prevenção à lavagem de dinheiro, as contrapartes com quem venha negociar os ativos que pretende adquirir, visando uma eficaz prevenção de quaisquer atividades inidôneas em seus ativos sob gestão.

## **8.3. Pessoas politicamente expostas**

Os procedimentos para a identificação e negociação com pessoas consideradas politicamente expostas (“PPE”) são tratados na Instrução CVM nº 301/99 e na Lei nº 9.613/98, e alterações posteriores, e demais normas editadas pelo BACEN, Conselho Monetário Nacional e GAFI/FATF.

O Artigo 3º-B da Instrução CVM nº 301/99 define a PPE como aquela que “desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo”.

Incluem-se os ocupantes de cargo, emprego ou função pública relevante exercido por chefes de estado e de governo, políticos de alto nível, altos servidores dos poderes públicos, magistrados ou militares de alto nível, dirigentes de empresas públicas ou dirigentes de partidos políticos. Também se recomenda a fiscalização de familiares da



PPE, seus parentes, na linha direta, até o primeiro grau, assim como o cônjuge, companheiro e enteado (Artigo 3º-B da Instrução CVM nº 301/99).

A Circular do BACEN nº 3.461, de 24 de julho de 2009, e alterações posteriores, dispõe sobre os procedimentos a serem observados pelos agentes financeiros para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras de PPE, os quais devem ser estruturados de forma a possibilitar a caracterização de pessoas consideradas PPE e identificar a origem dos fundos envolvidos nas transações dos Clientes assim identificados.

Recomenda-se aos sujeitos obrigados a especial, reforçada e contínua atenção no exame e cumprimento das medidas preventivas, sobretudo no que se refere às relações jurídicas mantidas com PPE, nos seguintes termos:

- (i) Supervisão de maneira mais rigorosa a relação de negócio mantido com PPE;
- (ii) Dedicção de especial atenção a propostas de início de relacionamento e a operações executadas com PPE, inclusive as oriundas de países com os quais o Brasil possua elevado número de transações financeiras e comerciais, fronteiras comuns ou proximidade étnica, linguística ou política;
- (iii) Manutenção de regras, procedimentos e controles internos para identificação de Clientes que se tornaram após o início do relacionamento com a instituição ou que seja constatado que já eram PPE no início do relacionamento com a instituição e aplicar o mesmo tratamento dos itens acima; e
- (iv) Manutenção de regras, procedimentos e controles internos para identificação da origem dos recursos envolvidos nas transações dos Clientes e dos beneficiários identificados como PPE.

Adicionalmente, recomenda-se a observação de outros fatores de risco, antes da aprovação de uma conta de PPE:

- (i) Transparência da fonte do dinheiro e dos bens para assegurar que estes não resultaram de recursos do Estado;
- (ii) Avaliação se a finalidade da conta e o nível de atividade proposto estão de acordo com o perfil financeiro geral da pessoa;
- (iii) Cargo político atual ou anteriormente exercido e sua duração;



- (iv) O nível de acesso da PPE a fundos estatais;
- (v) Avaliação da transparência e da complexidade da estrutura e da posse da conta; e
- (vi) O regime político e socioeconômico do país de origem, seu nível de corrupção e controle de drogas.

#### **8.4. Comunicações**

Se algum Colaborador perceber ou suspeitar da prática de atos relacionados à lavagem de dinheiro ou outras atividades ilegais por parte de qualquer Cliente, este deverá imediatamente reportar suas suspeitas ao Diretor de *Compliance*, que deverá, então, instituir investigações adicionais, para determinar se as autoridades relevantes devem ser informadas sobre as atividades em questão. Entre outras possibilidades, uma atividade pode ser considerada suspeita se:

- (i) operações cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial ou financeira de qualquer das partes envolvidas, tomando-se por base as informações cadastrais respectivas;
- (ii) operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;
- (iii) operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de qualquer das partes envolvidas;
- (iv) operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;
- (v) operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- (vi) operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);
- (vii) operações realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico;

- (viii) operações com a participação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo - GAFI;
- (ix) operações liquidadas em espécie, se e quando permitido;
- (x) transferências privadas, sem motivação aparente, de recursos e de valores mobiliários;
- (xi) operações cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do Cliente ou de seu representante;
- (xii) depósitos ou transferências realizadas por terceiros, para a liquidação de operações de Cliente, ou para prestação de garantia em operações nos mercados de liquidação futura;
- (xiii) pagamentos a terceiros, sob qualquer forma, por conta de liquidação de operações ou resgates de valores depositados em garantia, registrados em nome do Cliente;
- (xiv) situações em que não seja possível manter atualizadas as informações cadastrais de seus Clientes;
- (xv) situações e operações em que não seja possível identificar o beneficiário final; e
- (xvi) situações em que as diligências para identificação de pessoas politicamente expostas não possam ser concluídas.

A Gestora deverá dispensar especial atenção às operações em que participem as seguintes categorias de Clientes:

- (i) clientes não-residentes, especialmente quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador;
- (ii) clientes com grandes fortunas geridas por áreas de instituições financeiras voltadas para clientes com este perfil (*private banking*); e
- (iii) pessoas politicamente expostas.

A Gestora deverá analisar as operações em conjunto com outras operações conexas e que possam fazer parte de um mesmo grupo de operações ou guardar qualquer tipo de relação entre si.

Os Colaboradores não devem divulgar suas suspeitas ou descobertas em relação a qualquer atividade, para pessoas que não sejam o Diretor de *Compliance*. Qualquer contato entre a Gestora e a autoridade relevante sobre atividades suspeitas deve ser feita somente pelo Diretor de *Compliance*. Os Colaboradores devem cooperar com o Diretor de *Compliance* durante a investigação de quaisquer atividades suspeitas.

A Gestora deve manter atualizados os livros e registros, incluindo documentos relacionados a todas as transações ocorridas nos últimos 5 (cinco) anos, podendo este prazo ser estendido indefinidamente pela CVM, na hipótese de existência de processo administrativo.

O Diretor de *Compliance* deve assegurar que a Gestora previna qualquer danificação, falsificação, destruição ou alteração indevida dos livros e registros por meio de adoção de métodos necessários e prudentes.

Consideram-se operações relacionadas com terrorismo ou seu financiamento aquelas executadas por pessoas que praticam ou planejam praticar atos terroristas, que neles participam ou facilitam sua prática, bem como por entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas e as pessoas ou entidades que atuem sob seu comando.

## **9. ENVIO DE INFORMAÇÕES ÀS AUTORIDADES GOVERNAMENTAIS**

As leis e regulamentações brasileiras exigem que o gestor de investimentos entregue informações periódicas e/ou informações eventuais relacionadas à sua atividade de gestão e distribuição de ativos nos mercados de capitais do Brasil. Algumas destas informações serão apresentadas à CVM ou ANBIMA e outros serão apresentados às companhias em que os fundos de investimento (ou outro veículo de investimento) investem ou aos cotistas desses fundos de investimento.

Estas informações incluem, sem limitação, (i) as comunicações previstas na Instrução CVM 358, sobre posições detidas nas companhias que integram as carteiras dos veículos de investimento, nos termos ali especificados; (ii) atualização anual do formulário de referência, conforme exigido pelo artigo 15 da Instrução CVM 558, o qual contém, sem limitação, informações sobre os fundos geridos, valores sob gestão e tipos de investidores; (iii) revisão periódica de seus manuais, códigos e políticas, os quais devem ser disponibilizados no website da Gestora; e (iv) informações exigidas pela legislação e regulamentação que trata da prevenção à lavagem de dinheiro.

## **10. PROCEDIMENTOS OPERACIONAIS**

A Gestora atua em conformidade com os padrões e valores éticos elevados, principalmente observando e respeitando as normas expedidas pelos órgãos reguladores e suas Políticas Internas. Na condução de suas operações, a Gestora deverá:

- (i) observar o princípio da probidade na condução de suas atividades;
- (ii) prezar pela capacitação para o desempenho das atividades;
- (iii) agir com diligência no cumprimento das ordens, observado o critério de divisão das ordens (quando for o caso);
- (iv) obter e apresentar aos seus clientes informações necessárias para o cumprimento das ordens;
- (v) adotar providências para evitar a realização de operações em situação de conflito de interesses, assegurando tratamento equitativo a seus clientes; e
- (vi) manter, sempre, os documentos comprobatórios das operações disponíveis, tanto para os órgãos fiscalizadores, como para os investidores, pelos prazos legais.

### **10.1. *Registro de operações***

As operações serão registradas nos sistemas dos administradores fiduciários dos fundos de investimento cujas carteiras sejam geridas pela Gestora e no sistema da Gestora com o intuito de controlar e conferir as carteiras disponibilizadas por estes administradores.

### **10.2. *Liquidação das Operações***

As operações serão liquidadas pelos próprios fundos de investimentos, obedecidos os critérios estabelecidos pelos administradores fiduciários e instituições financeiras onde as operações foram realizadas.

## **11. PLANO DE CONTINUIDADE DO NEGÓCIO**

Na execução de suas atividades, a Gestora está sujeita a riscos relacionados à ocorrência de eventos que possam comprometer, dificultar ou mesmo impedir a continuidade das

operações da Gestora, tais como catástrofes naturais, ataques cibernéticos, sabotagens, roubos, vandalismos e problemas estruturais.

Este plano de continuidade do negócio busca descrever os procedimentos, estratégias, ações e infraestrutura empregados pela Gestora para garantir a continuidade das suas atividades em situações de contingência.

O responsável pelo cumprimento do plano de continuidade do negócio e pela ativação do plano de contingência é o Diretor de *Compliance*.

### **11.1 Estrutura e procedimentos de contingência**

A Gestora garantirá a continuidade de suas operações no caso de um desastre ou qualquer outra interrupção drástica dos negócios.

Os servidores da Gestora são virtuais, mantidos em nuvem (Google) com backup de 30 (trinta) dias, de forma que todas as informações podem ser acessadas remotamente de qualquer lugar com acesso à internet.

Em caso de emergência na sede da Gestora que impossibilite o seu uso, os Colaboradores terão o acesso remoto feito por navegadores de internet, pelo *software Google file stream*. Os colaboradores farão acesso utilizando de suas credenciais individuais, de acordo com as permissões pré-estabelecidas.

Todos os colaboradores possuem uma cópia do plano de continuidade do negócio que descreve todas as ações a serem seguidas em caso de desastre.

### **11.2 Plano de contingência**

O plano de contingência será acionado toda vez que, por qualquer motivo, o acesso às dependências da Gestora fique inviabilizado.

Nesses casos, o Diretor de *Compliance* deve determinar aplicação dos procedimentos de contingência.

Nos casos de impossibilidade de acesso à Gestora, os Colaboradores serão autorizados pelo Diretor de *Compliance* a trabalharem remotamente, no ambiente residencial do Colaborador ou em lugar a ser definido na oportunidade, o qual possua conexão própria e segura, sendo utilizando o notebook da Gestora, de modo a manterem o regular exercício de suas atividades.

Após a normalização do acesso à Gestora, os Colaboradores deverão apresentar ao Diretor de *Compliance* relatório das atividades executadas durante o período de contingência.

### 11.3 Atualização do plano de continuidade do negócio

Os procedimentos, estratégias e ações constantes do plano de continuidade do negócio serão testados e validados, no mínimo, a cada 12 (doze) meses, ou em prazo inferior, se exigido pela regulamentação em vigor.

## 12. SEGURANÇA CIBERNÉTICA

A Gestora adota mecanismos de segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é o Diretor de *Compliance*.

### 12.1. Avaliação dos riscos

No exercício das suas atividades, a Gestora poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

- i) *Malwares*: softwares desenvolvidos para corromper computadores e redes:
  - a. Vírus: software que causa danos à máquina, rede, outros softwares e bancos de dados;
  - b. Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
  - c. *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
  - d. *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
  
- ii) Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
  - a. *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - b. *Phishing*: links transmitidos por e-mails, simulando se ruma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

- c. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
  - d. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
  - e. Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- iii) Ataques de DDoS (*distributed denial of services*) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; 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.

## 12.2. Ações de prevenção e proteção

Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, a Gestora adota as seguintes medidas de prevenção e proteção:

- i) Controle de acesso adequado aos ativos da Gestora, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos da Gestora;
- ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis;
- iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;
- iv) Rotinas de *backup*;
- v) Criação de logs e trilhas de auditoria sempre que permitido pelos sistemas;
- vi) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que necessário, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;
- vii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais; e

viii) Restrição à instalação e execução de *softwares* e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

Nesse sentido a Gestora contratou os serviços de segurança cibernética da empresa de TI Informatizo, a qual utiliza o servidor de arquivo Google File Stream e Backup em nuvem Google de 30 (trinta) dias, sendo possível o gerenciamento de acesso individualizado às pastas dos respectivos Colaboradores.

Adicionalmente, a Gestora possui sistema de *firewall* Mikrotik e antivírus Itbrain, além de sistema *anti spam* nos e-mails corporativos e no servidor.

## **Monitoramento**

A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Gestora mantém inventários atualizados de *hardware* e *software*, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou softwares não licenciados.

Além disso, a Gestora mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de *backup* são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente, testes de invasão externa e *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a Gestora analisa regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

### **12.3. Plano de resposta**

Caso seja identificado um potencial incidente relacionado à segurança cibernética, o Diretor de *Compliance* deverá ser imediatamente comunicado.

Num primeiro momento, o Diretor de *Compliance* se reunirá com os demais diretores da Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.



Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, as medidas imediatas de cibersegurança cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, serão observados os procedimentos previstos no plano de continuidade do negócio, descrito no item 12 acima.

Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (iii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

#### **12.4. Reciclagem e revisão**

A Gestora manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

O Diretor de *Compliance*, responsável pela implementação dos procedimentos de segurança cibernética, realizará a revisão e atualização deste plano de segurança cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

**ANEXO I - Modelo de Relatório Anual de *Compliance***

São Paulo, \_\_\_\_\_ de janeiro de \_\_\_\_\_.

**Aos Diretores,**

*Ref.: Relatório Anual de Compliance*

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos **PANDHORA INVESTIMENTOS LTDA** (“Gestora”), nos termos do Manual de Controles Internos (*Compliance*) da Gestora (“Manual de Compliance”), e do Artigo 22 da Instrução nº 558, de 26 de março de 2015 da Comissão de Valores Mobiliários (“Instrução CVM 558”), e na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de *Compliance* e da Instrução CVM 558 (“Diretor de Compliance”), informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20\_\_\_\_.

Por favor, encontrem abaixo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de deficiências e cronogramas de saneamento; e (iii) minha manifestação, na qualidade de responsável por ajustar a exposição a risco das carteiras da Gestora, assim como pelo efetivo cumprimento da “Política de Gestão de Riscos” da Gestora, a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

- I. Conclusão dos exames efetuados:
- II. Recomendações e cronogramas de saneamento:
- III. Manifestação sobre verificações anteriores:

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

---

Leandro Alves da Silva  
Diretor de *Compliance* e Risco

## ANEXO II - Termo de Adesão

Eu, ....., portador da Cédula de Identidade nº ..... e Cadastro de Pessoas Físicas (CPF) nº ....., declaro para os devidos fins que:

1. Estou ciente da existência do “Manual de Controles Internos (*Compliance*)” da **PANDHORA INVESTIMENTOS LTDA.** (“Manual de Compliance” e “Gestora”, respectivamente) e de todas as políticas internas da Gestora, inclusive o “Código de Ética”, a “Política de Investimento Pessoal” e a “Política de Gestão de Risco” (“Políticas Internas”), que recebi, li e tenho em meu poder.
2. Tenho ciência do inteiro teor do Manual de *Compliance* e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual de *Compliance*), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela Gestora, e comprometo-me a comunicar, imediatamente, aos diretores da Gestora qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.
3. Tenho ciência e comprometo-me a observar integralmente os termos da política de confidencialidade estabelecida no Manual de *Compliance* da Gestora, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.
4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pela Gestora e/ou os respectivos sócios e diretores, oriundos do não-cumprimento do Manual de *Compliance* e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.
5. Participei do processo de integração e treinamento inicial da Gestora, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Gestora, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.
6. As normas estipuladas no Manual de *Compliance* e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pela Gestora, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.

7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei a Gestora a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual de *Compliance*, salvo conflitos decorrentes de participações em outras empresas, descritos na “Política de Investimento Pessoal”, os quais tenho ciência que deverão ser especificados nos termos previstos no Manual de *Compliance*:

---

---

---

---

---

---

---

---

---

---

---

Local e data:

---

Assinatura:

---

**ANEXO III - Solicitação para Desempenho de Atividade Externa**

1. Nome da instituição na qual será realizada a Atividade Externa / descrição da Atividade Externa: \_\_\_\_\_

2. Você terá uma posição de diretor ou administrador?  sim  não

3. Descreva suas responsabilidades decorrentes da Atividade Externa: \_\_\_\_\_

4. Tempo estimado que será requerido de você para desempenho da Atividade Externa (em bases anuais): \_\_\_\_\_

5. Você ou qualquer parte relacionada irá receber qualquer remuneração ou contraprestação pela Atividade Externa:  sim  não

Se sim, descreva: \_\_\_\_\_

O Colaborador declara que a Atividade Externa que pretende desempenhar, conforme acima descrita, não viola nenhuma lei ou regulamentação aplicável, ou os manuais e códigos da **PANDHORA INVESTIMENTOS LTDA.** (“Gestora”), e que não interfere com suas atividades na Gestora, não compete ou conflita com quaisquer interesses da Gestora. O Colaborador declara e garante, ainda, que irá comunicar ao diretor de *Compliance* da Gestora quaisquer conflitos de interesses que possam surgir com relação à Atividade Externa acima descrita.

São Paulo, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_\_\_\_.

\_\_\_\_\_  
[Colaborador]

Resposta do Diretor de *Compliance*:  Solicitação Aceita  Solicitação Negada

\_\_\_\_\_  
Leandro Alves da Silva - Diretor de *Compliance*

