REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

Porto Alegre, 07 de maio de 2021.

Rua Cândido Silveira, 198, 6º Andar
Auxiliadora, Porto Alegre, RS
90540-010

harbourcapital.com.br

SUMÁRIO

1. PROCEDIMENTOS E CONTROLES INTERNOS (COMPLIANCE)

1.1 Considerações Gerais

A área de Compliance da Harbour Capital é responsável pela elaboração e manutenção do Programa de Compliance da Gestora, que inclui a revisão e atualização periódica das Políticas internas, bem como a implementação de controles internos e testes de aderência para monitorar a efetividade das mesmas e, ainda, a realização de treinamentos aos Colaboradores que possuem acesso a informações confidenciais, participem do processo de decisão de investimento ou participem do processo de distribuição de cotas de fundos de investimento.

A Gestora, no exercício de suas atividades, deve garantir, por meio de controles internos adequados, o permanente atendimento às normas, políticas e regulamentações com vistas a dar cumprimento às obrigações estabelecidas na Instrução CVM n. 558/15, bem como demais normas, diretrizes e Ofícios de Orientação emitidos pelos referidos órgãos, dentre outras melhores práticas nacionais e internacionais, referentes às diversas modalidades de investimento, às atividades de gestão e aos padrões ético e profissionais.

Esta Política objetiva, portanto, disciplinar a atuação da área de Compliance da Gestora, esclarecendo suas responsabilidades e os procedimentos a serem observados quando de sua atuação. Assim, nos termos da Instrução CVM n. 558/15, artigo 14, inciso III, a presente Seção estabelece as regras, procedimentos e controles internos para o cumprimento da referida instrução.

1.2 Deveres do Diretor de Compliance e da Área de Compliance e Risco

O Diretor de Compliance e Risco é o responsável por implementar regras, políticas, procedimentos e controles internos da Gestora, bem como por garantir o cumprimento destas, da Instrução CVM n. 558/15 e outras normas aplicáveis à Gestora, coordenando a Área de Compliance e Risco nas respectivas atribuições desta.

Portanto, as principais obrigações da Área de Compliance e Risco, sem prejuízo das atribuições exclusivas do Diretor de Compliance e Risco constantes nas normas aplicáveis ou neste Código ou nas demais políticas da Gestora, são as seguintes:

I. estabelecer princípios éticos e regras de conduta e efetuar alterações neste Código sempre que entender necessário aperfeiçoamentos ou complementações a tais princípios éticos e regras de condutas;

II. divulgar este Código e demais políticas da Gestora, através da entrega de cópias físicas ou eletrônicas, treinamento inicial e treinamentos periódicos aos Colaboradores que atuem na gestão e que tenham ou possam vir a ter acesso a Informações Confidenciais, conforme acima previsto;

III. fiscalizar e acompanhar regras previstas neste Código e em outras políticas da Gestora;

IV. receber pedidos de autorização, orientação ou esclarecimento, conforme acima previsto, bem como tomar as respectivas providências (inclusive, mas não se limitando, as que envolvam Conflitos de Interesses e tratamento de Informações Confidenciais);

V. receber denúncias sobre a ocorrência, suspeita ou indício de práticas em desacordo com este Código ou com demais normas aplicáveis à Gestora, bem como tomar as devidas providências;

VI. acessar e compilar dados e informações, mapear os processos de Compliance, fazer revisões periódicas dos processos de Compliance e aprimorá-los em razão de alterações de normas aplicáveis, do modelo de negócios ou porte da Gestora, ou qualquer outra razão;

VII. fazer avaliações periódicas de questões estratégicas ou gerenciais em conjunto com as demais áreas, para testar a eficiência dos controles para gerenciamento de riscos, buscando melhorar o desempenho por meio de revisão de processos e da elaboração de planos de ação, nos moldes do Formulário Modelo em anexo a este Manual;

VIII. dar suporte no que se refere à interpretação e impacto da legislação, monitorando as melhores práticas em sua execução, e analisar as normas emitidas pelos órgãos reguladores, tais como a CVM e o Banco Central do Brasil ("BACEN"), informando as áreas e departamentos relevantes;

IX. cumprir as obrigações relativas ao combate aos crimes de lavagem ou ocultação de bens, direitos e valores e outros ilícitos;

X. solicitar o apoio da auditoria interna ou externa ou outros assessores profissionais, sempre que necessário, visando a efetividade deste Código e o devido cumprimento de leis e normas aplicáveis à Gestora; e

XI. aplicar eventuais sanções aos Colaboradores que descumprirem este Código.

Sempre que entender necessário ou conveniente, o Diretor de Compliance poderá levar qualquer assunto de sua competência para apreciação ou deliberação pelo Comitê de Compliance.

2. CONTROLE DE INFORMAÇÕES CONFIDENCIAIS

2.1 Políticas De Confidencialidade

A Diretoria Executiva-Operacional controla o cumprimento das políticas internas de segurança da informação, segurança cibernética e continuidade dos negócios, para manter o nível de segurança das informações produzidas e obtidas pela Harbour Capital no desenvolvimento de suas atividades em patamar definido como adequado, assegurando os seguintes princípios norteadores:

I. **Confidencialidade:** Proteção compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo, permitindo que sejam expostos voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

II. **Integridade:** Garantia da veracidade de dados, pois estes não devem ser alterados enquanto estão sendo transferidos ou armazenados. Ameaça à segurança acontece quando um determinado dado (físico ou não) fica exposto ao manuseio por uma pessoa não autorizada, que efetua divulgações e/ou alterações não aprovadas e sem o controle de seu proprietário (corporativo ou privado).

III. **Disponibilidade e Continuidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As

ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

IV. **Acesso controlado:** O acesso dos usuários a dados é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

2.2 Políticas de Segurança

Nesta sessão são descritos os procedimentos de segurança para os sistemas de informações confidenciais, não apenas, mas em especial para os mantidos em meio eletrônico, pelo menos por parte de seus sócios, administradores, colaboradores e dos funcionários que a possuem.

I. **Controle de acesso físico a documentos confidenciais:** Arquivos físicos, papéis e documentos são mantidos em uma área protegida da Gestora, cujo acesso é controlado. O escritório da Harbour Capital é trancado e requer autorização para acesso.

II. **Controle de acesso pessoal:** Informações confidenciais somente são acessadas por Colaboradores que necessitem ter acesso a tais informações para desempenhar uma atividade de negócios em nome da Harbour Capital. Além disto, sempre é possível identificar os detentores dessas informações para responsabilização, em caso de vazamento.

III. **Controle de acesso a arquivos eletrônicos:** Computadores e pastas eletrônicas são protegidas por login e senha individualizado, e apenas as pessoas previamente autorizadas podem acessá-los. O acesso a informações confidenciais é limitado a determinados Colaboradores cuja necessidade é justificada.

IV. **Restrições de discussão:** Colaboradores ou departamentos afetados devem abster-se de discutir em áreas públicas ou com pessoas de fora do departamento (incluindo familiares, amigos, etc.) quaisquer atividades que não sejam publicamente conhecidas.

V. **Monitoramento de comunicações:** Ao assinar o Termo de Compromisso da Harbour Capital, o Colaborador concorda em autorizar o Diretor Executivo-Operacional e o

Diretor de Compliance a monitorar comunicações e atividades envolvendo os trabalhos por ele executados no âmbito profissional.

VI. **Medidas de controle de acesso externo:** O site da Harbour Capital é protegido por firewalls, um servidor seguro e programas de antivírus. Funcionários são proibidos de fazer downloads de informações sensíveis. Somente em circunstâncias excepcionais, funcionários podem ser autorizados a trabalhar fora do escritório e durante este período a rede da Harbour Capital será acessada remotamente. O acesso remoto é protegido e controlado. Testes de invasão e "fishing test" são feitos periodicamente. O uso de pendrives é expressamente proibido.

3. APROVAÇÃO DE PRESTADORES DE SERVIÇOS, PARCEIROS E COLABORADORES

A Harbour Capital prima por proteger sua reputação e, para isso, é imprescindível que apenas contrate colaboradores, negocie com players e contrate prestadores de serviços que possuam reputação ilibada, bem como qualificação/certificação compatível com as atividades que são por eles realizadas.

Com esse intuito, a área de Compliance estabelece procedimentos de aprovação de novos parceiros, prestadores de serviços e colaboradores, e auxilia as áreas devidas no processo de análise destes, os quais deverão ser observados pela Diretoria Executiva-Operacional, responsável pelo processo de seleção e contratação de prestadores de serviços, parceiros e colaboradores.

3.1 Aspectos gerais

O uso de fornecedores terceirizados permite que a Harbour Capital foque nas na gestão do portfólio de seus fundos e negócios enquanto faz uso dos recursos da maneira mais eficiente possível. Ao escolher um fornecedor externo, diversos fatores serão considerados dependendo do tipo de serviço fornecido. Fatores que podem ser considerados ao envolver um terceiro incluem, mas não são limitados a:

I. Período de tempo no negócio e reputação;

II. Estabilidade financeira;
III. Conhecimento prévio do fornecedor;
IV. Outros usuários dos serviços do fornecedor;
V. Tecnologia e habilidade de entregar os serviços;
VI. Segurança do cliente e outras informações financeiras, se aplicável;

3.2 Consultores financeiros qualificados

A Harbour Capital poderá contratar consultores externos para auxiliar em sua avaliação de investimentos potenciais e existentes, especificamente para fornecer pesquisa e/ou informações relativas a indústrias e/ou empresas. Para escolher tais fornecedores, fatores como reputação, qualidade da informação entregue e avaliação global das práticas de segurança de informação do fornecedor serão avaliadas.

3.3 Uso de terceiros para distribuição

Os fundos da Harbour Capital poderão fazer uso de agentes autônomos e distribuidores terceirizados ("Distribuidores Terceirizados") para captação de recursos. Para isso, a Harbour Capital aceitará abrir mão de receita de taxas de administração ou performance ("Rebates").

A Harbour Capital poderá auxiliar o administrador de seus fundos a selecionar Distribuidores Terceirizados. Para escolhê-los, serão utilizados como critério fatores como reputação, histórico de atuação, portfólio de clientes, análise das políticas de relacionamento e estratégia de captação, qualidade do trabalho desenvolvido e feedback de clientes.

Não serão contratados agentes autônomos, lobistas, advogados ou consultores com o propósito de aproximar ou intermediar contato com autoridade, executivo, funcionário ou fiduciário de regimes públicos de previdência social ou regimes de previdência complementar.

4. APROVAÇÃO DE PRODUTOS, SERVIÇOS E NEGÓCIOS

A área de Compliance deverá, sempre que necessário e solicitada pelo Comitê de Investimentos ou pelo Diretor Executivo-Operacional, participar ativamente da análise de novos produtos e serviços a serem fornecidos e de novos negócios a serem realizados pela

Harbour Capital, observando, sobretudo, eventuais riscos inerentes aos produtos/serviços/negócios em questão e eventuais ajustes nas regras, políticas e controles internos advindos dos novos produtos e/ou serviços.

O objetivo é auxiliar na prevenção de dilemas/conflitos de interesse e evidenciar os pontos sensíveis, bem como tratar eventuais problemas, suportando as tomadas de decisões internas. A Gestora preocupa-se em evitar circunstâncias que possam produzir conflito de interesses, seja em situação de colisão de interesses da Gestora com os dos Colaboradores, seja com os dos Clientes. Em caso de dúvida, o potencial conflito de interesse deverá ser levado ao conhecimento do Comitê de Compliance, que definirá a linha de ação a ser tomada.

5. PRECIFICAÇÃO

A Harbour Capital reconhece a importância de avaliar adequadamente todos os recursos dos fundos de investimento e de desenvolver políticas e procedimentos apropriados. Com relação a qualquer fundo de investimento, a Harbour Capital estabeleceu políticas e procedimentos de *valuation* designados em coerência com metodologias de *valuation* estabelecidos em documentos organizacionais.

Os gestores de carteiras da Harbour Capital não devem ter autoridade exclusiva na determinação do valor dos títulos para os quais não haja mercado prontamente disponível (cotação), mas podem assistir na análise de *valuation* justa. Sob nenhuma circunstância os gestores de carteiras terão a capacidade de controlar ou iniciar alterações nos preços. Como uma nota prática, a Harbour Capital delegou a *valuation* de valores mobiliários e ativos ao administrador dos fundos.

Em consulta com os membros do Comitê de Investimentos da Harbour Capital e, quando necessário, do Comitê de Compliance, o administrador será responsável tanto por determinar quanto por aprovar qualquer *valuation* de valores mobiliários, respondendo por qualquer conduta que infrinja este ou qualquer outro Manual que regule a atuação da empresa e de seus colaboradores, em especial seu Código de Ética.

6. TREINAMENTOS

6.1 Política Geral

A política de treinamentos da Harbour Capital tem como objetivo estabelecer as regras que orientem o treinamento de administradores, empregados e colaboradores que possuam acesso a informações confidenciais e participem do processo de decisão de investimento, de forma a torná-los aptos a seguir todas as regras dispostas nas Políticas.

Todos os colaboradores devem receber o devido treinamento acerca de todas as políticas e procedimentos constantes deste Manual, o qual deve abranger as políticas e procedimentos adotados pela Harbour Capital e deve ser compatível com a atividade desempenhada pelo administrador, funcionário ou colaborador. Assim, será proporcionado aos Colaboradores uma visão geral das Políticas adotadas, de forma que se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas

A área de Compliance será responsável por organizar e promover as sessões de treinamento aos administradores, empregados e colaboradores de forma que estes entendam e cumpram as disposições previstas nas políticas da empresa. A metodologia, os materiais, carga horária e grade horária serão definidos pela área de Compliance e poderão incluir, mas não se limitando a, sessões expositivas (presencial ou de forma remota), estudos de caso e testes de compreensão dos conceitos, rotinas e procedimentos previstos nas políticas da Gestora.

O treinamento será realizado a cada 12 (doze) meses, e obrigatório a todos os Colaboradores. Quando do ingresso de um novo colaborador, a Diretoria aplicará o devido treinamento de forma individual para o novo colaborador. A Diretoria poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às Políticas ou sempre que ocorrer modificação das premissas norteadoras do Manual de Compliance da Harbour Capital. O treinamento obrigatoriamente incluirá elementos do programa de lavagem de dinheiro e tratamento de informações confidenciais.

A Gestora poderá financiar cursos de aprimoramento profissional aos Colaboradores, principalmente aos membros da equipe técnica, desde que julgue viável e interessante o conteúdo. O controle e a supervisão das práticas profissionais dos Colaboradores visarão

promover a aplicação conjunta da referida Política com as normas estabelecidas nas demais políticas aprovadas nos termos do presente Manual.

6.2 Certificação profissional

O Colaborador deverá informar o Diretor Executivo-Operacional se possui qualquer certificação profissional relacionada às atividades que desenvolve na Harbour Capital. A Diretoria Executiva-Operacional é responsável pela manutenção dos registros eletrônicos nas autoridades competentes relativamente aos Colaboradores cuja certificação é necessária.

7. ESTABELECIMENTO DE CANAIS DE COMUNICAÇÃO

A Harbour Capital possui um canal de denúncias interno e externo, destinado aos seus colaboradores e público externo, para que enviem suas críticas, sugestões, reporte de ocorrências e, sobretudo, denúncias de práticas que firam a filosofia da instituição, suas políticas e manuais, e a regulamentação, legislação e/ou autorregulação aplicável.

Caso o informante esteja diante de alguma prática, ou suspeite do exercício de alguma prática que viole as diretrizes ou quaisquer das políticas e procedimentos deste Manual, deverá informar a área de Compliance por meio do canal apropriado. A comunicação pode ser realizada ao endereço eletrônico compliance@harbourcapital.com.br. Alternativamente, é disponibilizado canal que garante o anonimato nos casos em que os colaboradores prefiram não se identificar, no sítio eletrônico https://share.hsforms.com/1niMoSs1xRUq8XXjbl7wJ6gbnwfz.

Vale ressaltar que a informação obtida por meio de qualquer canal é considerada confidencial, deve ser tratada com sigilo e não pode ser, de nenhuma forma, utilizada para prejudicar seu portador, garantindo, dessa forma, a privacidade do informante e permitindo que ele se sinta confortável para fazer uso dos meios de comunicação da Gestora.

8. SEGREGAÇÃO DE ATIVIDADES

Considerando a atuação da Harbour Capital na gestão de Fundos, a independência das áreas é garantida por meio da segregação lógica de todas as áreas envolvidas nas atividades da Harbour Capital, com a criação de perfis de usuários para a rede interna e para o sistema

interno (cada colaborador somente possui acesso aos documentos necessários para a boa execução de suas funções – “need to know” basis).

No que tange o seu objeto social, caso a Harbour Capital venha desenvolver outra atividade no mercado de capitais, além da gestão de recursos de terceiros, essa nova atividade deverá ser totalmente segregada das atividades atualmente realizadas, salvo no que for expressamente permitido pela legislação e pela regulamentação em vigor.

Por ora, tendo em vista que as atividades da Harbour Capital estão concentradas unicamente na gestão de recursos de terceiros, nos termos da Instrução CVM n. 558/15, não há necessidade de segregação física de pessoal, somente segregação eletrônica, que ocorre por meio de acessos limitados ao conteúdo de cada departamento.

9. SEGURANÇA DA INFORMAÇÃO

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Harbour Capital, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Instrução CVM n.º 558/15 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a Harbour Capital procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade (“Informações Confidenciais”), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Harbour Capital, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Harbour Capital, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou demais órgãos caso autorizado pelo Diretor de Risco e Compliance.

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de

serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

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

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- Malware – softwares desenvolvidos para corromper computadores e redes:
- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações; e
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- 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.

- 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.
- Invasões (advanced persistent threats) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Harbour Capital pode estar sujeita a problemas de funcionalidade dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais Os planos de ação e prevenção descritos neste Capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a Harbour Capital ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da Harbour Capital, evitando o acesso por terceiros não autorizados.

Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreiras da informação eventualmente existentes.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo reportados imediatamente qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Diretor Executivo-Operacional. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

São adotadas as seguintes medidas preventivas para os riscos identificados: backup, firewalls e antivírus, bem como análise de prestadores de serviço e adoção de cláusulas de confidencialidade.Periodicamente são realizadas verificações, a fim de identificar elementos estranhos à Harbour Capital, tais como computadores e acessos não autorizados.O monitoramento dos controles existentes e estabelecidos nessa Política podem ser realizados e executados por empresa subcontratada, sob supervisão da Diretoria Executiva-Operacional.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Gestora esteja preparada para a continuação de suas atividades, assim como para mitigar eventuais riscos operacionais ou reputacionais.

10. POLÍTICA DE PREVENÇÃO E GESTÃO DE CONFLITO DE INTERESSES

Os colaboradores deverão atentar para a existência de situações que possam ensejar conflitos entre os interesses (i) da Harbour Capital e dos clientes/investidores, (ii) de colaborador(es) e dos clientes/investidores; ou (iii) entre os próprios clientes/investidores.

Como padrão usual de diligência e supervisão, a Harbour Capital espera que seus colaboradores levem ao conhecimento da Área de Compliance quaisquer riscos notados e/ou preocupações quanto a determinadas práticas comerciais conduzidas pela instituição ou por quaisquer de seus colaboradores. Caso seja verificado algum possível conflito de interesse relacionado às atividades desenvolvidas pela Harbour Capital, seus colaboradores e prestadores de serviços, bem como em relação a prestadores e contrapartes dos fundos de investimentos por ela geridos, a área de Compliance deve seguir o procedimento abaixo:

I. entender a situação com as partes envolvidas;
II. entender quais são os interesses em jogo e se o é um caso de conflito real ou em potencial;
III. verificar formas de dirimir o conflito ou, se não for possível, de ao menos mitigá-lo; e
IV. escalar as discussões para a instância superior competente, sempre que julgar necessário.

11. POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DE TERRORISMO (“PLD/CFT”)

Os fundos geridos pela Sociedade contarão com administradores idôneos e que possuam Políticas próprias de Conhecimento do Cliente, Suitability, bem como de Prevenção e Combate à Lavagem de Dinheiro. Sem prejuízo, sempre que a atividade de distribuição for realizada internamente, a Sociedade promoverá tais processos internamente.

Serão registrados e informados ao Comitê de Investimentos se, na análise cadastral do cliente, houver suspeita quanto à sua atividade econômica/financeira; e/ou se identificada

pessoa politicamente exposta; e/ou se identificada pessoa envolvida em prática de atos dispostos na Lei n. 12.846/13 (Lei Anticorrupção); e/ou se identificado processos judiciais e administrativos em que o cliente/investidor seja ou tenha sido parte, sua natureza e resultado, bem como a relevância de tais informações para o relacionamento com o cliente e para as boas práticas do mercado.

Serão orientadas as áreas envolvidas na atividade a supervisionar de maneira rigorosa as operações e relações mantidas por pessoas consideradas politicamente expostas, conforme definição outorgada pela legislação aplicável ao tema. A Sociedade atentará, de maneira efetiva, quando da proposição e realização de operações, se há indícios de crime, ou suspeitas de atividades ilícitas. No documento "Política De Prevenção à Lavagem De Dinheiro", estão descritas situações em que a Harbour Capital se compromete em manter vigilância.

A não observância dos dispositivos da presente Política resultará em advertência, suspensão ou demissão/exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais, bem como conforme definido no Código de Ética de Conduta da Sociedade.

12. DESCUMPRIMENTO DE MANUAIS, POLÍTICAS, LEGISLAÇÃO, AUTORREGULAÇÃO E REGULAMENTAÇÃO VIGENTES POR COLABORADORES

O desrespeito e/ou o descumprimento deste Manual, dos demais manuais e políticas internos, bem como da legislação, autorregulação e regulamentação vigentes por qualquer colaborador da Harbour Capital, podem levar, dependendo da gravidade e/ou reincidência da violação, à aplicação de medidas punitivas, seja no âmbito da própria Harbour Capital (advertências, suspensão do contrato de trabalho ou demissão por justa causa, expulsão da sociedade), seja no âmbito penal, civil ou trabalhista.

Estes casos devem ser apreciados pela área de Compliance que levará sua recomendação à Diretoria Executiva-Operacional, podendo até, se necessário, ser reportados à autoridade competente, sendo certo que tais questões devem ser tratadas dentro do mais absoluto sigilo de modo a preservar os interesses e a imagem da Harbour Capital, dos eventuais denunciantes e dos eventuais colaboradores envolvidos, exceto nos casos de necessidade de testemunho judicial ou em manifestação em processo administrativo.

Rua Cândido Silveira, 198, 6º Andar
Auxiliadora, Porto Alegre, RS
90540-010

harbourcapital.com.br

Anexo I

TERMO DE ADESÃO AO MANUAL DE COMPLIANCE DA HARBOUR CAPITAL

TERMO DE ADESÃO AO MANUAL DE COMPLIANCE DA HARBOUR CAPITAL

Eu, _____, inscrito(a) no CPF/MF sob o n. _____, na qualidade de _____ (cargo) da Harbour Capital, pelo presente instrumento, atesto que recebi, li e entendi o Manual de Compliance da Harbour Capital e confirmo que tenho conhecimento integral de todas as Políticas e procedimentos aqui constantes.

Comprometo-me a cumpri-lo integralmente e fazer cumprir a quem me incumbir, no que for aplicável, confirmando minha ciência acerca das sanções aplicáveis a cada um dos casos de violação das Políticas constantes deste Manual.

Data:

Assinatura:

Anexo II

Modelo-Base para Relatório Anual de Compliance e PLDFT

Aos Sócios e Diretores da Harbour Capital.

Assunto: Relatório Anual de Compliance e PLDFT

Tendo em vista a previsão constante do Manual de Compliance e PLDFT da Harbour Capital, é anualmente realizada a revisão, atualização e eventual correção das regras, políticas, procedimentos, controles internos e a avaliação interna de risco de LDFT da HARBOUR CAPITAL ADMINISTRADORA DE CARTEIRAS DE VALORES MOBILIARIOS LTDA., observando-se o disposto no artigo 22 da Instrução CVM n. 558/15 e no artigo 6º da Instrução CVM n. 617/19.

Por esta razão, na qualidade de diretor responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos, controles internos e PLDFT encaminho à V. Sas. o presente relatório, demonstrando os resultados os exames efetuados, as eventuais recomendações de ajustes/melhorias, o cronograma para sua implementação e o acompanhamento da aplicação de recomendações realizadas em relatórios e/ou comunicações anteriores.

O presente relatório se refere ao exame do período compreendido entre 1º de janeiro e 31 de dezembro de 20xx e as suas conclusões podem ser encontradas nos tópicos abaixo.

Relatório de Compliance, políticas e controles internos:

Conclusão dos exames efetuados no período de referência:
Recomendações de melhoria, atualização e/ou correções das políticas de compliance:
Cronograma de implementação das recomendações:

Follow-up de recomendações de períodos anteriores:
Outras considerações relevantes:

Relatório relativo às Políticas de Lavagem de Dinheiro e ao Financiamento do Terrorismo:

Política de KYC, identificação de beneficiários finais, cadastros e manutenção/atualização das informações:	
Atuação de prepostos, AAI e terceirizados:	
Dados consolidados do ano-base:	
a) número de operações/situações atípicas detectadas:	
b) número de análises realizadas:	
c) número de comunicações de operações suspeitas reportadas:	
d) a data do reporte da declaração negativa, se for o caso:	
Indicadores de efetividade:	
Recomendações a serem implementadas:	

Sendo o que tínhamos para o momento, toda a equipe da Diretoria de Compliance permanece à disposição para prestar os esclarecimentos eventualmente necessários.

Porto Alegre, xx de xxxxxx de 20xx.

_____

Diretor de Compliance