REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

(Manual de Compliance)

HARBOUR
CAPITAL

Histórico de versões:		
Versão	**Modificação**	**Data**
05	Revisão Anual	11/12/2023
Data de vigência: 20 de dezembro de 2023		
Público: Interno e Externo		

SUMÁRIO

1. PROCEDIMENTOS E CONTROLES INTERNOS (MANUAL DE 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, a implementação de controles internos, a realização de testes de aderência para monitorar a sua efetividade e a realização de treinamentos aos colaboradores.

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 Resolução CVM n. 21/21, bem como demais normas e melhores práticas nacionais e internacionais, referentes às diversas modalidades de investimento, às atividades de gestão e aos padrões éticos e profissionais.

Esta Política objetiva disciplinar a atuação da área de Compliance da Gestora, esclarecendo suas responsabilidades e os procedimentos a serem observados quando de sua atuação e estabelecer as regras, procedimentos e controles internos.

1.2 Deveres do Diretor e da área de Compliance

O Diretor de Compliance e Risco é o responsável por implementar regras, políticas, procedimentos e controles internos da Gestora e garantir o seu cumprimento, coordenando a área de Compliance nas suas respectivas atribuições. As principais obrigações da área de Compliance, sem prejuízo daquelas constantes nas normas aplicáveis ou nas demais políticas da Gestora, são as seguintes:

I. estabelecer princípios éticos e regras de conduta e efetuar alterações neste Manual sempre que entender necessário aperfeiçoamentos ou complementações;
II. divulgar este Manual e demais políticas da Gestora, através da entrega de cópias físicas ou eletrônicas, treinamento inicial e treinamentos periódicos aos colaboradores;
III. fiscalizar e acompanhar regras previstas neste Manual e em outras políticas da Gestora;
IV. receber pedidos de autorização, orientação ou esclarecimento, conforme acima previsto, bem como tomar as respectivas providências;

V. receber denúncias sobre a ocorrência, suspeita ou indício de práticas em desacordo com este Manual e às demais políticas da Gestora, em especial sobre PLDFT, bem como tomar as devidas providências;

VI. 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 (Anexo II);

VII. 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 a Anbima, informando as áreas e departamentos relevantes;

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

IX. solicitar o apoio da auditoria interna ou externa ou outros assessores profissionais sempre que necessário, visando a efetividade deste Manual e o devido cumprimento de leis e normas vigentes, aplicando eventuais sanções aos colaboradores que descumprirem as Políticas da Gestora.

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, o qual se reunirá, ordinariamente, semestralmente e, extraordinariamente, sempre que convocado pelo Diretor de Compliance. Suas decisões serão tomadas por maioria simples de votos.

2. SELEÇÃO E MONITORAMENTO DE PRESTADORES DE SERVIÇOS

A Harbour Capital prima por proteger sua reputação e, para isso, é imprescindível que apenas contrate colaboradores e 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, responsável pelo processo de seleção e contratação de prestadores de serviços, parceiros e colaboradores.

O uso de fornecedores terceirizados permite que a Harbour Capital foque na gestão do portfólio de seus fundos 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. Os fatores que devem ser considerados ao envolver um terceiro dependem da análise interna de risco da contratação (a depender da área e da exposição decorrente dessa contratação) e incluem, mas não são limitam a: período de tempo no negócio e reputação; estabilidade financeira; conhecimento prévio do fornecedor; tecnologia e habilidade de entregar os serviços; segurança do cliente e outras informações financeiras, se aplicável; existência de políticas próprias, tais como Código de Ética e Conduta , Manual Compliance, Política Anticorrupção e/ou adequação às políticas de segurança da informação; manuais próprios de monitoramento de processos com devida adequação à normas legais e de proteção de dados pessoais; feedback de outros usuários dos serviços do fornecedor. Maiores informações constam do procedimento interno para seleção e acompanhamento de prestadores serviços, em linha com a Resolução CVM n. 175/22.

Para a contratação de serviços de administração fiduciária, a Harbour conta com processo específico, o qual leva em consideração fatores como sistemas disponibilizados para extração de informações, tempestividade das informações para controle dos ativos, zeragem automática, SLAs para atendimento de demandas, sistema de atualização de cotas; bem como questões relativas à operação de Fundos Estruturados, quando for o caso.

Os fundos da Harbour Capital poderão fazer uso de agentes autônomos e distribuidores terceirizados para captação de recursos. Para isso, a Gestora poderá renunciar a parte da receita de taxas de administração ou performance e 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, feedback de clientes, certificações obtidas, dentre outros.

3. APROVAÇÃO E ESTRUTURAÇÃO DE NOVOS PRODUTOS

A Harbour Capital conta com Comitê de Estruturação, composto por um representante da Diretoria Executiva/Comercial, um representante da área de Gestão, e um representante da área de Compliance e Risco. Possui como suas principais atribuições:

- deliberar sobre a aprovação de novos produtos;
- definir responsáveis (internos ou terceiros contratados) pela estruturação;
- identificar e propor mecanismos de mitigação de riscos dos novos produtos;
- quando deliberar favoravelmente pela estruturação de novos produtos, definir, minimamente: as diretrizes da política de investimentos, os hard e soft limits para controle de risco e os prestadores de serviços recomendados para contratação;
- sugerir, quando for necessário, ajustes nas regras, políticas e controles internos advindos dos novos produtos e/ou serviços;
- identificar e propor medidas para prevenir conflitos de interesse, sendo que, em caso de dúvida, o potencial conflito deverá ser levado ao conhecimento do Comitê de Compliance, que definirá a linha de ação a ser tomada.

O Comitê de Estruturação possui caráter não-permanente e se reúne sempre que convocado pelo Diretor Executivo, tomando suas decisões por unanimidade.

4. POLÍTICA DE CERTIFICAÇÃO, TREINAMENTOS E QUALIFICAÇÃO

4.1 Política de Certificação

A Harbour Capital segue as melhores práticas de certificação e capacitação técnica dos profissionais que atuam em suas áreas chaves.

A área de Compliance é responsável pela manutenção e atualização dos registros eletrônicos nas autoridades competentes relativamente aos colaboradores cuja certificação é necessária (notadamente o sistema de Certificação/RH da Anbima), bem como pelo monitoramento do prazo para sua renovação e ou alteração das condições necessárias às suas atividades. Para fins de identificação de todos os profissionais certificados, cada colaborador deverá informar à área de Compliance se possui qualquer certificação profissional relacionada às atividades que desenvolve na Harbour Capital.

Sendo identificada a necessidade de obtenção/atualização de certificação profissional para o desenvolvimento de qualquer atividade pela Harbour Capital, o colaborador receberá apoio da Gestora para obtenção da certificação correta. No caso de qualquer colaborador estar ocasionalmente desempenhando atividade que demande certificação específica e que este não a possua, ou a tenha vencida, este será afastado das funções dependentes da certificação até que a obtenha/renove.

Estão dispensados das regras desta seção os colaboradores da área administrativa e outras áreas que desempenham atividades acessórias à gestão de recursos, salvo disposição legal em contrário.

4.2 Política de Treinamentos e Qualificação dos Colaboradores

A política de treinamentos da Harbour Capital tem como objetivo estabelecer as regras que orientem o treinamento de administradores 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 novos colaboradores devem receber o devido treinamento acerca de todas as políticas da Harbour Capital. 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. Periodicamente, são realizados programas de reciclagem, recertificações e seminários sobre assuntos relacionados às atividades da Gestora.

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 online), 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 é obrigatório a todos os colaboradores. Quando do ingresso de um novo colaborador, será aplicado de forma individual para o novo colaborador. A área de Compliance 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. Referido treinamento indicará as principais mudanças nas Políticas da Harbour e incluirá elementos do programa de lavagem de dinheiro, Código de Ética, tratamento de informações confidenciais e conflito de interesses.

É dever de todo colaborador participar dos treinamentos obrigatórios, devendo a eventual ausência ser justificada para a área de Compliance, com a posterior realização de treinamento em outra data.

Todos os colaboradores são encorajados a participar de palestras, seminários, congressos, cursos, dentre outros eventos relacionados à sua área de atuação e da Gestora, a fim de manter-se atualizado com as melhores práticas adotadas pelo mercado. Igualmente, lhes é oferecido uma gama de cursos de habilidades básicas para sua atividade profissional, os quais estão elencados em documento próprio na rede da Gestora.

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. CANAIS DE COMUNICAÇÃO E DENÚNCIAS

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 o Código de Ética da Gestora, suas políticas e manuais, 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/denunciantes prefiram não se identificar, no endereço 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 forma alguma utilizada para prejudicar seu portador, garantindo a privacidade do informante no uso dos meios de comunicação da Gestora.

7. 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 os sistemas internos (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.

8. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança de Informação 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 Resolução CVM n. 21/21 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a Harbour Capital procura identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade, 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 Compliance e Risco.

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. Pode ocorrer também por ligação telefônicas (*vishing) e/ou por mensagens de texto e aplicativos de mensagem (smishing);*

- 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; e
- Invasões (*advanced 11ersistente threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

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 a perda e/ou adulteração de dados e informações confidenciais. Os planos de ação e prevenção descritos neste Manual tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

No caso de suspeita sobre a autenticidade de determinada comunicação, link, site, etc., interromper à operação e comunicar à área de Compliance ou, alternativamente ao Diretor Executivo. No caso de suspeita de perda de dados, acesso não autorizado ou roubo de informações, interromper imediatamente as atividades e reportar à área de Compliance.

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 reportada qualquer inconsistência ou inadequação de acesso, de forma automática e imediata, pela solução tecnológica adotada pela Gestora para armazenamento de dados, serviço de e-mail e videochamadas. Especial atenção deverá ser dispensada nos casos de férias de colaboradores e no seu desligamento, caso em que o acesso deve ser revogado imediatamente.

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 área de Compliance.

Todos os documentos arquivados nos computadores da Harbour Capital são objeto de back-up periódico, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

Os testes de contingência são 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.

8.1 Política De Confidencialidade e Proteção de Informações

Os colaboradores da Harbour Capital que tiverem acesso aos sistemas de informação, serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos. Todos os computadores utilizados pelos colaboradores da Harbour Capital possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas. Adicionalmente, todas as mensagens enviadas/recebidas nos e-mails eletrônicos de propriedade da Harbour Capital permitem a identificação do seu remetente/receptor.

O controle e o cumprimento das políticas internas de segurança da informação, segurança cibernética e continuidade dos negócios é de responsabilidade da Diretoria Executiva e busca 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, buscando evitar a quebra de sigilo que permita a exposição 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. Devem ser evitadas situações em

que 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, incluindo métodos de garantir a disponibilidade dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança, evitando que informação deixe 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 possam obtê-la, evitando descuidos ou possível quebra da confidencialidade das senhas de acesso à rede e/ou às dependências da gestora.

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

Informações adicionais sobre tratamento de informações confidenciais podem ser encontradas no Código de Ética da Harbour Capital.

8.2 Políticas de Segurança

A Harbour Capital adota controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação. 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.

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, por parte de administradores, colaboradores e dos funcionários que as possuem.

I. **Controle de acesso físico a documentos confidenciais:** arquivos físicos, papéis e documentos são mantidos em áreas segredadas e protegidas da Gestora, cujo acesso

é controlado. A sede da Harbour Capital possui medidas para restrição de acesso e qualquer ingresso requer autorização prévia.

II. **Controle de acesso pessoal:** informações confidenciais somente são acessadas por colaboradores que necessitem ter acesso a tais informações para desempenhar suas atividades. Além disto, os mecanismos de controle de acesso permitem a identificação dos detentores das informações para responsabilização.

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 aos colaboradores cuja necessidade de conhecimento seja decorrente de suas atividades, sendo controlado pela área de compliance em arquivo próprio e atualizado periodicamente.

IV. **Restrições de discussão:** colaboradores ou departamentos afetados devem se abster 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 Adesão ao Manual de Compliance da Harbour Capital, o colaborador autoriza a Gestora a monitorar as comunicações e atividades envolvendo os trabalhos por ele executados no âmbito profissional, sendo altamente recomendável que todas as comunicações referentes às atividades desenvolvidas sejam realizadas dentro do sistema da Gestora.

VI. **Medidas de controle de acesso externo:** A rede da Harbour Capital (armazenamento, e-mails, videochamadas) é provida por reconhecido prestador de serviços de tecnologia, sendo os computadores autorizados dotados de programas de antivírus e softwares licenciados. Colaboradores são orientados a não realizar download de informações sensíveis e podem ser autorizados a trabalhar fora do escritório, sendo que neste caso a rede da Harbour Capital será acessada remotamente. O acesso remoto é protegido e controlado. O uso de pendrives é expressamente proibido.

Todos os programas de computador utilizados pelos colaboradores devem ser originais, respeitar os direitos de propriedade intelectual pertinentes e estar de acordo com a política de segurança da informação. À exceção dos softwares já aprovados para instalação e

listados na rede interna da Gestora, downloads de qualquer natureza podem ser realizados, desde que de forma justificada e devidamente autorizados.

Informações adicionais acerca das zonas de restrição de acesso à informação, boas práticas, solicitações de acesso e demais orientações procedimentais podem ser encontradas no arquivo '*Processos de controle de acessos*', disponível na rede interna da Gestora.

9. 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.

Informações adicionais sobre conflito de interesses podem ser encontradas no Código de Ética da Gestora.

10. PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO - PLDFT

A Harbour Capital possui Política de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo que estabelece as regras, processos e controles a serem aplicados e seguidos

no desenvolver de suas atividades, baseado em sua avaliação interna de risco e que prevê, dentre outras questões, as regras de KYC, a identificação de operações suspeitas e a forma de tratamento/comunicação destas.

Adicionalmente, os fundos geridos pela Sociedade contarão com administradores idôneos, aderentes às boas práticas da Anbima e que possuam Políticas próprias de conhecimento do cliente, *suitability* e PLDFT. Sem prejuízo, a Gestora tem processos estabelecidos para realizar esses controles internamente quando necessário.

Todas as áreas da Gestora são orientadas a supervisionar de maneira rigorosa as operações e relações mantidas por pessoas consideradas politicamente expostas, conforme sua definição legal. Os colaboradores atentarão, de maneira efetiva, quando da proposição e realização de operações, se há indícios de crime, ou suspeitas de atividades ilícitas.

A não observância dos dispositivos da 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, nos termos previstos no Código de Ética. Informações adicionais sobre PLDFT podem ser encontradas na Política específica.

11. DISPOSIÇÕES FINAIS E REVISÃO

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, podendo, 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.

A área de Compliance deverá manter todos os documentos e informações exigidos arquivados pelo prazo previsto na regulamentação vigente ou por prazo superior quando determinado pelos órgãos reguladores e autorreguladores, sendo admitido o arquivamento de forma digital.

Este Manual será revisado anualmente, podendo ser alterado a qualquer tempo em razão da identificação de circunstâncias que demandem sua atualização antecipada. O histórico de versões deste documento é o seguinte:

Histórico de versões:		
Versão	**Modificação**	**Data**
01	Criação	26/05/2020
02	Atualização	07/05/2021
03	Revisão Anual	29/10/2021
04	Revisão Anual	25/11/2022
05	Revisão Anual	11/12/2023

Dúvidas podem ser sanadas diretamente com a área de Compliance pelo e-mail compliance@harbourcapital.com.br.

ANEXO I – TERMO DE ADESÃO

TERMO DE ADESÃO AO MANUAL DE COMPLIANCE DA HARBOUR CAPITAL

Eu, _____,

inscrito(a) no CPF sob o n. _____, na qualidade de Colaborador(a)/Prestador(a) de Serviço da Harbour Capital, pelo presente instrumento, atesto que recebi, li e entendi o Manual de Compliance e de Controles Internos. Igualmente, confirmo que tenho conhecimento e entendimento integral de todas as Políticas, regras 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 DE RELATÓRIO ANUAL

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 na Política de 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 na Resolução CVM n. 21/21 e na Resolução CVM n. 50/21.

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 área de Compliance permanece à disposição para prestar os esclarecimentos eventualmente necessários.

Porto Alegre, xx de xxxxxx de 20xx.

_____

Diretor de Compliance