REDPOINT EVENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA.

Manual de Compliance

(Outubro de 2018)

I. Introdução

1. **REDPOINT EVENTURES GESTÃO DE RECURSOS E CONSULTORIA LTDA.**, sociedade limitada brasileira com sede na Cidade de São Paulo, Estado de São Paulo, na Alameda Vicente Pinzon, 54, andar 00, Vila Olímpia, CEP 04547-130, inscrita no CNPJ sob o nº 29.292.940/0001-83 ("**Redpoint**" ou "**Sociedade**"), por meio deste Manual de Compliance ("**Manual**"), define os meios pelos quais as infrações das políticas e os principais riscos operacionais podem ser monitorados e identificados.

2. Os controles internos da Redpoint se aplicam a todos os sócios, administradores, diretores, empregados e estagiários, bem como pessoas relacionadas, ou seja, pessoas físicas sobre as quais pode ser exercido qualquer tipo de influência em relação a suas atividades ("**Membros**").

3. Tais controles são realizados de acordo com práticas internacionais e locais, aplicando os procedimentos necessários para cumprir as disposições dos Artigos 19 e 21 da Instrução CVM nº 558/15, de 26.3.2015, com relação à: (a) implementação e manutenção de um programa de treinamento para Membros que têm acesso à informações confidenciais e/ou fazem parte dos processos de tomada de decisões de investimento; (b) acesso limitado a arquivos e implementação de controles que limitem e identifiquem as pessoas que têm acesso à informações confidenciais; (c) definição das políticas relacionadas à compra e venda de valores mobiliários por Membros da Redpoint; e (d) identificação e registro de clientes, de forma a evitar crimes de "lavagem de dinheiro", ou seja, aqueles tipificados principalmente na Lei n.º 9.613, de 3.3.1998, conforme alterada pela Lei nº 12.683, de 9.7.2012.

4. As políticas internas estão sujeitas a revisão e atualização anuais, por meio das quais passarão a incorporar medidas relativas a novos riscos ou a riscos não abordados anteriormente. Na hipótese de quaisquer dúvidas em relação a essas ou a quaisquer outras políticas e procedimentos da Redpoint, é preciso entrar em contato com o Departamento de Compliance e Gestão de Risco da Redpoint.

II. Objetivo

5. O objetivo deste Manual é garantir, juntamente com todas as outras políticas adotadas, a adequação, o fortalecimento e o funcionamento do sistema de controle interno da Redpoint, na tentativa de minimizar os riscos de acordo com a complexidade das operações do negócio e

de disseminar a cultura de controle de modo a garantir o cumprimento com as leis e os regulamentos em vigor.

6. Os benefícios de cumprimento com as leis e os regulamentos em vigor são vários e incluem uma maior capacidade de a Redpoint atender as necessidades dos clientes e de garantir uma maior competitividade, à luz da transparência e da ética com a qual a Sociedade conduz seu negócio. Os custos de descumprimento das normas de *compliance* são altos e incluem danos à reputação da Redpoint, a rescisão de licenças operacionais e diversas sanções, incluindo o ajuizamento de processos administrativos e criminais, além de multas. Portanto, todos os Membros da Sociedade têm acesso às políticas internas da Redpoint e recebem instruções contínuas sobre os métodos de cumprimento com tais políticas.

III. A Responsabilidade e as Atividades para a Promoção do Compliance

7. Em decorrência da implementação de atividades de *compliance* em sua estrutura, o responsável pelo Departamento de Compliance e Gestão de Risco da Redpoint será o Sr. Fábio Schenberg Frascino, que atuará em sinergia com o Departamento Técnico, de modo a garantir a definição correta dos objetivos da Redpoint, emitindo normas, regulamentos e diretrizes a todos os Membros.

8. Um programa de *compliance*, como o estabelecido pela Sociedade, pode desempenhar um papel central no monitoramento de riscos relacionados às atividades de gestão de ativos. O cumprimento com as leis, os regulamentos, as políticas internas e os processos de controle, os documentos contábeis dos clientes e princípios fiduciários sólidos é essencial para a Redpoint. Garantir esse cumprimento é uma função importante do responsável pela área de *compliance*.

9. O Departamento de Compliance e Gestão de Risco da Redpoint terá como principais funções prestar assistência a todas as áreas em termos de esclarecimentos, instruções e cumprimento com todos os controles e regulamentos internos, bem como supervisionar a conformidade das operações e das atividades da Sociedade com as leis e os regulamentos aplicáveis. Entre as principais funções, devem ser destacadas as seguintes:

(i) *Estabelecimento de políticas*: Administrar a implementação das políticas e dos procedimentos de *compliance* dentro da Sociedade; atualizar essas políticas, procedimentos e o Manual em linha com as alterações nas leis, nos regulamentos e nas diretrizes; coordenar os esforços de *compliance* da Redpoint; estabelecer procedimentos para revisão anual de seus programas de *compliance*; disseminar manuais, procedimentos e políticas de *compliance* e quaisquer outras informações relacionadas a *compliance* dentro da Sociedade; estabelecer, manter e implementar políticas e procedimentos designados a: (a) cumprir todas as leis, regulamentos e diretrizes relevantes; (b) detectar e impedir violações; e (c) denunciar quaisquer violações substanciais e/ou medida corretiva recomendada.

(ii) *Autorizações e aprovações*: Garantir que a Redpoint celebre apenas acordos, contratos ou qualquer outro tipo de documento quando a contraparte tenha sido devidamente autorizada e tenha recebido os poderes necessários para celebrar esses acordos, contratos ou outros documentos.

(iii) *Comunicação*: Identificar situações que envolvem conflito de interesses e informar todas e quaisquer ocorrências de tais situações ou qualquer outro tipo de informação que possa ser razoavelmente necessária.

(iv) *Avaliação de risco*: Estabelecer, manter e implementar políticas adequadas para avaliação, monitoramento e gestão de riscos, bem como procedimentos para identificar e avaliar a exposição a possíveis riscos. Além disso, o profissional deverá garantir que os riscos assumidos pela Sociedade sejam monitorados constantemente e que medidas adequadas de minimização de riscos sejam tomadas.

(v) *Cumprimento de formalidades*: Garantir que os contratos celebrados pela Sociedade sejam, em todos os momentos, celebrados e devidamente estabelecidos de acordo com a forma jurídica aplicável em cada caso e que todas e quaisquer operações envolvendo recursos de terceiros sejam devidamente documentadas por meio de instrumentos legais relevantes.

(vi) *Confidencialidade*: Garantir que todos os dados relacionados ao principal negócio da Redpoint sejam mantidos no mais absoluto sigilo, exceto à luz de autorização ou regulamentação que obrigue a Sociedade a divulgar tais informações.

(vii) *Treinamento*: Atualizar e supervisionar constantemente os Membros da Sociedade com relação às políticas de *compliance* e de controle interno da Redpoint, e ser receptivo às ideias e propostas apresentadas pelos Membros para a melhoria da Sociedade.

IV. Critérios para Implementação de Compliance

10. A Redpoint manterá uma avaliação contínua da eficácia de controles internos a respeito das normas estabelecidas. De acordo com essa avaliação, a Sociedade utilizará critérios objetivos, a saber: (i) *Ambiente de controle*: define o estilo da organização, influenciando a consciência de controle do pessoal. Essa é a base para todos os outros componentes de controles internos; (ii) *Avaliação de risco*: identificação e análise de riscos relevantes que afetam o alcance dos objetivos, fornecendo uma base a respeito de como a gestão de riscos deve ser conduzida; (iii) *Informação e controle*: sistemas ou processos que fornecem assistência para a identificação, coleta e troca de informações, dentro de cronogramas que permitam às pessoas físicas realizarem suas funções; (iv) *Controle das atividades*: políticas e

procedimentos que ajudam a garantir que as diretrizes da administração sejam seguidas; (v) *Acompanhamento*: processos utilizados para avaliar a qualidade do desempenho de controles internos com o tempo.

11. Com base na avaliação decorrente dos critérios mencionados, a Redpoint verificará com frequência se suas políticas de controle interno estão atingindo seus objetivos esperados. Caso ocorram quaisquer alterações, seja na estrutura regulatória ou em suas práticas administrativas, a Sociedade informará todos os Membros sobre tais alterações e fornecerá à sua equipe treinamento adicional.

V. Princípios Básicos e Conduta Ética

12. A Sociedade atuará como administradora de carteiras, uma vez que esteja devidamente credenciada pela Comissão de Valores Mobiliários ("**CVM**"). O relacionamento fiduciário exige aderência aos mais altos padrões de conduta e de integridade.

13. Os Membros devem cumprir suas obrigações para o benefício exclusivo dos clientes. Consistente com essa obrigação fiduciária, os interesses dos clientes têm prioridade sobre os objetivos de investimentos pessoais e sobre os outros interesses pessoais dos Membros da Redpoint. Dessa forma:

(i) Os Membros devem trabalhar para eliminar, ou minimizar, conforme a Política de Negociação de Valores Mobiliários da Redpoint, qualquer conflito ou indício de conflito entre os interesses próprios de qualquer pessoa física coberta pelo Manual e a responsabilidade dela perante nossos clientes ou perante a Redpoint; e

(ii) Os Membros nunca devem utilizar indevidamente seus cargos na Sociedade para ganhos pessoais próprios, de sua família ou de qualquer outra pessoa.

14. O negócio da Redpoint está sujeito a uma estrutura jurídica e regulatória. Assim, nossas atividades comerciais devem, por lei, satisfazer um padrão de conduta maior que o esperado em muitos outros tipos de negócios. O presente Manual e demais políticas da Sociedade resumem os valores, princípios e práticas que orientam nossas atividades, orientando todos os Membros da Redpoint a respeito das exigências mínimas que se espera que sejam cumpridas. Todos os Membros devem ler o Manual e demais políticas da Redpoint, certificarem-se de que entenderam seu conteúdo e comprometer-se em cumprir suas disposições. Uma vez lido o Manual, o Membro ingressante na Sociedade deverá preencher o termo de adesão (**Anexo I**), o qual deverá ser renovado, no mínimo, anualmente.

VI. Ouvidoria

15. A Redpoint estabeleceu o programa de Ouvidoria como um importante elemento na promoção de monitoramento, fornecendo um mecanismo seguro para os Membros buscarem orientação sobre como denunciar ou resolver problemas relacionados ao trabalho. O ouvidor é uma parte neutra e independente, disponível a todos os Membros da Sociedade. A Ouvidoria fornece um recurso confidencial e alternativo no qual o Membros pode discutir de forma segura e sigilosa suas preocupações relacionadas ao trabalho. A função do ouvidor não substitui o trabalho da administração da unidade e de outros canais formais de resolução de problemas. Em vez disso, o ouvidor complementa e suplementa esses canais formais. Os Membros podem discutir qualquer tipo de problema relacionado ao trabalho com o ouvidor, incluindo possível má conduta financeira, violações de nosso Manual ou das políticas da Redpoint, bem como outros problemas a respeito do trabalho individual, do ambiente de trabalho ou de conflito interpessoal. Apesar do ouvidor não ter autorização para aceitar ou para receber notificação de reivindicações e não conduz investigações, o ouvidor pode ajudar na discussão e na avaliação de todas as opções de denúncia. Em caso de dúvida acerca do programa de Ouvidoria dos Membros da Redpoint, o Departamento de Compliance e Gestão de Risco da Redpoint deverá ser contatado.

VII. Denúncia de Conflitos, Problemas e Violações

16. É de responsabilidade de cada Membro ser sensível às situações e aos relacionamentos que poderão criar conflitos de interesses e trazer quaisquer perguntas ou preocupações relacionadas ao Departamento de Compliance e Gestão de Risco da Redpoint, conforme elas surgirem. Essa obrigação de denunciar abrange não só conflitos entre Membros e clientes da Redpoint, ou entre a Sociedade e seus clientes, mas também conflitos que poderão surgir entre os interesses de um cliente e de outro cliente ou de um grupo ou classe de clientes e de outro grupo ou classe de clientes. O Departamento de Compliance e Gestão de Risco da Redpoint determinará o método mais apropriado de lidar com o conflito denunciado, conforme a Política de Negociação de Valores Mobiliários da Redpoint. Isso poderá exigir a implementação de controles ou de procedimentos. O Departamento de Compliance e Gestão de Risco da Redpoint deve ser consultado antes da implementação de quaisquer alterações a esses controles ou procedimentos.

17. Além disso, os Membros devem denunciar imediatamente quaisquer violações conhecidas das políticas da Redpoint ao Departamento de Compliance e Gestão de Risco da Redpoint, bem como quaisquer violações que acreditarem razoavelmente que estejam prestes a ocorrer. Caso esse método de denúncia não seja apropriado ou caso o Membro não se sinta confortável em fazê-lo, o problema poderá ser levado ao conhecimento à Ouvidoria. O ouvidor está à disposição dos Membros para levarem preocupações sobre questões comerciais da Redpoint que entendam implicar em matérias de ética ou práticas questionáveis. O ouvidor

fornecerá orientação confidencial e sigilosa de forma segura e resolve questões problemáticas relacionadas ao trabalho. No entanto, a função do ouvidor não substitui a função da administração e de outros canais formais de resolução de problemas.

18. A Redpoint tem uma política rigorosa de combate à retaliação. Nenhum Membro poderá realizar qualquer ação retaliatória contra qualquer Membro que (i) fornece informações ou auxilia em investigações de violações de lei de segurança ou combate à fraude ou (ii) inicia, depõe ou participa, ou de outra forma auxilia nos processos que envolvem supostas violações de leis ou de regulamentos de combate à fraude.

VIII. Conflitos Pessoais, Ações Disciplinares e Finanças

19. A Redpoint identificou vários conflitos de interesses em seu negócio e desenvolveu políticas e procedimentos para abordá-los. Contudo, os relacionamentos pessoais dos Membros também poderão gerar conflitos com os interesses de clientes, da Sociedade ou de seus sócios. Todos os Membros devem denunciar todos os referidos conflitos ao Departamento de Compliance e Gestão de Risco da Redpoint.

20. Além disso, devido à natureza do negócio da Redpoint, espera-se que todos os Membros administrem suas finanças pessoais de forma que não afete negativamente suas responsabilidades na Sociedade ou gere uma publicidade desfavorável à Redpoint. Ademais, uma situação financeira precária pode ser considerada uma influência sobre ações ou julgamentos feitos em nome da Sociedade de uma forma inapropriada. Adicionalmente, em reconhecimento da importância em particular de Membros que alinham seus próprios interesses pessoais com os interesses dos clientes da Redpoint, os Membros são incentivados a utilizar os produtos e os serviços oferecidos pela Sociedade, conforme disponíveis e apropriados, nos termos da Política de negociação de valores mobiliários da Redpoint.

IX. Pagamento e Recebimento de Valores

21. O pagamento e recebimentos de valores recebidos pela Redpoint, na qualidade de distribuidora de fundos sob sua gestão, segue todos os padrões estabelecidos pela Instrução CVM n° 505, de 27.9.2011 ("**Instrução CVM n° 505**"), inclusive com relação aos arquivos a serem mantidos com relação a tais operações, conforme artigo 30 desta Instrução.

22. A Redpoint, nos termos do artigo 32 da Instrução CVM n° 505, se compromete a, por meio de seus sistemas e políticas internas:

(a) zelar pela integridade e regular funcionamento do mercado, inclusive quanto à seleção de clientes e à exigência de garantias;

(b) manter controle das posições dos clientes, com a conciliação periódica entre ordens e posições, conforme inciso II do artigo mencionado;

(c) manter registro de conta corrente de todas as movimentações financeiras de seus clientes;

(d) informar à CVM sempre que verifique a ocorrência ou indícios de violação da legislação que incumba à CVM fiscalizar, no prazo máximo de 5 (cinco) dias úteis da ocorrência ou identificação;

(e) informar seus clientes sobre os produtos oferecidos e seus riscos;

(f) informar seus clientes com relação aos mecanismos de ressarcimento de prejuízos estabelecidos pelas entidades administradoras de mercado organizado, se for o caso;

(g) diferenciar nas notas de corretagem, faturas e avisos de lançamento enviados aos clientes, os valores decorrentes de corretagem daqueles relativos a outros serviços prestados pelo intermediário e das taxas e emolumentos cobrados pelas entidades administradoras de mercado organizado ou por outros terceiros, se for o caso; e

(h) suprir seus clientes com informações e documentos relativos aos negócios realizados na forma e prazos estabelecidos em suas regras internas.

23. O diretor responsável, Sr. Romero Venâncio Rodrigues Filho, deverá assegurar que tais procedimentos serão realizados na atividade de distribuição das cotas dos fundos de investimento geridos pela Redpoint.

X. Práticas de Combate à Corrupção

24. A Redpoint está totalmente comprometida com o cumprimento de todas as leis de combate à corrupção sempre que conduzir o negócio. Dessa forma, a Sociedade proíbe a realização de qualquer pagamento a qualquer pessoa que atue em qualquer capacidade para obter ou manter negócio de forma ilícita ou de outra forma para garantir uma vantagem imprópria. Para garantir a conformidade:

(i) Nenhum Membro da Redpoint deverá, em nenhuma circunstância, oferecer, prometer ou autorizar qualquer pagamento ou benefício a um funcionário do governo ou a qualquer pessoa para os fins de induzir o funcionário do governo a agir ou abster-se de agir com relação ao cumprimento de suas obrigações oficiais, principalmente se a ação ou omissão do funcionário do governo puder resultar na obtenção ou manutenção do negócio ou na garantia de uma vantagem comercial imprópria por parte da Sociedade; e

(ii) Todos os pagamentos feitos por ou em nome da Redpoint devem ser registrados de forma precisa, adequada e imediata em seus livros e registros contábeis.

25. Normalmente, é difícil determinar o ponto em que uma cortesia comercial oferecida à outra pessoa ultrapassa os limites do excesso e, em última instância, é considerada um suborno. Portanto, não poderão ser oferecidos entretenimentos ou presentes, nem viagens ou despesas com hotel poderão ser pagas a nenhum funcionário do governo, em nenhuma circunstância, sem a expressa autorização prévia por escrito (correspondência por e-mail é aceitável) dos membros do Departamento de Compliance e Gestão de Risco da Redpoint.

XI. Combate à Lavagem de Dinheiro

26. A Redpoint, diligentemente, toma precauções contra quaisquer tentativas de usar a Sociedade para depositar ou transferir recursos que possam estar relacionados com atividades ilegais. A lavagem de dinheiro é um processo pelo qual transgressores procuram dar aparência lícita a recursos provenientes de atividades ilegais, de maneira a aparentar que o dinheiro é de fonte legítima. A Redpoint implementou sua Política de Combate e Prevenção à Lavagem de Dinheiro, que deverá ser lida em conjunto com este Manual, bem como procedimentos razoavelmente desenvolvidos para evitar tais atividades e para se proteger contra qualquer prejuízo financeiro e responsabilidade legal relacionada.

27. Alguns princípios gerais a serem considerados:

(i) Nenhum Membro da Sociedade deve jamais participar, de maneira consciente, de qualquer operação financeira proibida ou, de maneira consciente, prestar assistência a qualquer cliente, sócio do negócio ou terceiros em violação de quaisquer leis e regulamentos de combate à lavagem de dinheiro aplicáveis. Esse princípio inclui a obrigação de evitar "cegueira deliberada", em que uma pessoa permite que uma operação obviamente ilícita passe desapercebida.

(ii) Os Membros devem conhecer suficientemente os clientes da Redpoint (*suitability*), a fim de assegurar que a Sociedade conduza o negócio apenas com empresas e pessoas físicas que atendam os padrões necessários para que a Redpoint possa cumprir, de maneira confortável, as suas exigências nos termos das leis e regulamentos de combate à lavagem de dinheiro aplicáveis. Isso inclui ter conhecimento da fonte dos recursos ou patrimônio dos clientes, quer o cliente realize operações ou resida em um país sujeito a programas de sanções mantidos por vários governos, quer o cliente conste de uma lista de pessoas restritas emitida por vários governos e pela ONU.

(iii) Todos os Membros, independentemente de seu cargo ou localidade, devem permanecer alerta para detectar possíveis atividades criminosas ou suspeitas e, imediatamente, denunciar operações questionáveis ao Departamento de Compliance e Gestão de Risco da Redpoint.

(iv) Na medida em que um registro relacionado a uma atividade suspeita aos padrões estabelecidos neste Manual e/ou na Política de Combate e Prevenção à Lavagem de Dinheiro da Redpoint for detectado, e em conformidade com a Lei n° 12,683 de 2012, o Membro irá registrar uma denúncia, conforme apropriado, perante a:

- CVM (Comissão de Valores Mobiliários do Brasil) http://www.cvm.gov.br/ingl/indexing.asp

- O Conselho de Controle de Atividades Financeiras ("COAF") (Banco Central do Brasil) https://www.coaf.fazenda.gov.br/conteudo-ingles/about-money-laundering

XII. Prevenção Contra Fraudes

28. A Sociedade tem o compromisso de estabelecer uma cultura organizacional que assegurará que a prevenção contra fraudes seja parte Membro de todas as atividades da Redpoint e uma responsabilidade fundamental de sua administração. Com relação a isso, a política de controle de fraudes da Sociedade:

(i) Especifica o compromisso da administração em identificar exposições a risco de atividades fraudulentas e estabelecer controles e procedimentos para a prevenção e detecção de tais atividades;

(ii) Exige que todos os Membros, administração e diretores abstenham-se de atividades fraudulentas e estimulem a denúncia de qualquer suspeita ou evento de fraude;

(iii) Fornece canais formais de denúncia em que os Membros podem relatar condutas e práticas impróprias que podem ser consideradas fraudulentas;

(iv) Exige investigação imediata e consistente das alegações de fraude interna, de acordo com a política de não retaliação, conforme especificado no presente Manual e demais políticas da Redpoint;

(v) Permite avaliação regular dos riscos de fraude e garante que toda atividade fraudulenta suspeita seja tratada de maneira apropriada e consistente; e

(vi) Fornece um programa de Ouvidoria disponível a todos os Membros.

29. Qualquer pessoa que suspeite de atividade fraudulenta deve notificar imediatamente o Departamento de Compliance e Gestão de Risco da Redpoint.

30. Todos os responsáveis pelos departamentos da Redpoint são responsáveis por assegurar que existam mecanismos em vigor, dentro de sua área de supervisão, para avaliar o risco de fraude, promover a consciência de ética dos Membros, orientá-los a respeito de prevenção/detecção de fraudes e manter uma estrutura de controle interno efetiva dentro de sua área de responsabilidade organizacional.

31. As políticas e práticas de recrutamento são uma parte importante da prevenção contra fraude e incluem: verificações de antecedentes criminais de todos os Membros novos e verificação de referências, registros de processos judiciais e de qualificação/licença, conforme aplicável pela legislação em vigor.

32. Tópicos relacionados à ética, conflitos, conduta do Membro, negociação pessoal e cumprimento de obrigações dos Membros fazem parte de programas e procedimentos contínuos de desenvolvimento, treinamento e conscientização dos Membros e do treinamento em ética/*compliance*.

XIII. *Suitability*

33. Além do cadastro dos clientes, realizado nos termos da Instrução nº CVM 505, serão conduzidos procedimentos de *suitability*, na forma da Instrução CVM nº 539, de 13.11.2013, conforme alterada, que permitam verificar a adequação dos produtos, serviços e operações ao perfil dos clientes por meio da elaboração e atualização periódica de perfil dos investidores, levando em conta sua capacidade financeira, conhecimento de finanças, qualificação e experiência em matéria de investimentos, seu objetivo de investimento e sua tolerância aos riscos.

34. O objetivo do procedimento de *suitability* é estabelecer procedimentos formais que possibilitem verificar a adequação do investimento realizado pelo cliente ao perfil de risco a ele atribuído, levando-se em consideração sua situação financeira, sua experiência em matéria de investimentos, grau de tolerância a volatilidade e os objetivos visados ao buscar os serviços da Redpoint, incluindo: (a) o entendimento do perfil, as expectativas, as restrições e os objetivos de investimento do Investidor de acordo com suas necessidades econômico-financeiras, presentes e futuras, observados padrões de risco, a necessidade de liquidez e o prazo de retorno; e (b) a prestação de serviços de seleção, alocação e realocação de patrimônio financeiro por meio da gestão de carteiras ou de fundos exclusivos e/ou restritos.

35. Para determinar o objetivo de investimento do cliente, a Redpoint deverá considerar: (a) o período pretendido de investimento; (b) as preferências declaradas do cliente em relação

à assunção de riscos; e (c) as finalidades do investimento.

36. Para definir a situação financeira do cliente, a Redpoint deverá considerar: (a) o valor das receitas regulares declaradas pelo cliente; (b) o valor que compõe o patrimônio do cliente; e (c) a necessidade futura de recursos declarada pelo cliente.

37. Para definir o conhecimento do cliente, a Redpoint deverá considerar (a) os tipos de produtos, serviços e operações com os quais o cliente tem familiaridade, (b) a natureza, volume e frequência, bem como o período das operações do cliente, e (c) a formação acadêmica e profissional do cliente.

38. O diretor responsável pelos procedimentos de s*uitability*, Sr. Romero Venâncio Rodrigues Filho, deverá assegurar que tais procedimentos serão realizados na atividade de distribuição das cotas dos fundos de investimento geridos pela Redpoint.

XIV. Reclamações de Clientes

39. Apesar dos melhores esforços da Redpoint e dos Membros, problemas com clientes e reclamações poderão ocorrer ocasionalmente e terão de ser tratados de maneira imediata, completa e profissional. Reclamações verbais ou escritas poderão ser feitas pelo cliente, pelo advogado ou representante do cliente, por uma autoridade regulatória ou outro terceiro. Reclamações poderão envolver o modo pelo qual uma operação foi realizada, precificada, registrada, ou liquidada; a gestão, administração, ou contabilidade de ativos; a base para remuneração e pagamentos, ou uma pessoa física ou jurídica que tenha sido aliciada ou consultada etc. Poderá haver uma exigência, expressa ou implícita, de pagamento ou outro recurso e, possivelmente, ameaça de ação regulatória, litígio ou perda do negócio.

40. As reclamações podem levar a qualquer um dos seguintes resultados possíveis: (i) um grave prejuízo financeiro para uma conta do cliente; (ii) perda do negócio; (iii) risco de ação regulatória ou litígio; ou (iv) dano à reputação. Qualquer pessoa que tenha conhecimento de uma possível ação ou receba diretamente uma notificação nesse sentido deve notificar imediatamente o Departamento de Compliance e Gestão de Risco da Redpoint.

XV. Troca de Informações com Administradores dos Fundos

41. A Redpoint e o administrador fiduciário dos fundos de investimento por ela geridos manterão procedimentos que garantam que a troca de informações ocorra de forma criptografada por meio de rede segura, de maneira que a Redpoint tenha acesso seguro aos documentos atualizados dos fundos e para que as áreas operacionais recebam as informações sobre aplicações e resgates de cotas dos fundos de investimento. Os procedimentos contemplam rotinas que garantem o fluxo de informações diariamente, com definição de

horários-limite para recebimento de instruções, meios de transmissão aceitos e prazos de arquivamento.

42. Na distribuição das cotas dos fundos geridos pela Redpoint serão observadas, conforme aplicável, as disposições dos artigos 17 e seguintes da Instrução CVM nº 555, de 17.12.2014 ("**Instrução CVM nº 555**"), que estabelece as normas aplicáveis às trocas de informações entre o distribuidor e o administrador do fundo de investimentos.

43. Ainda, caso autorizada a distribuição por conta e ordem pelo administrador fiduciário por parte da Redpoint, serão observados, em sua integralidade, os procedimentos descritos nos artigos 30 e seguintes da Instrução CVM nº 555, incluindo o estabelecimento, pela Redpoint, de registro complementar de cotistas que inscreva a titularidade das cotas em nome dos investidores, atribuindo a cada cotista um código de cliente e informando tal código ao administrador do fundo.

44. A responsabilidade pelo cumprimento das disposições aplicáveis da Instrução CVM nº 555 descritas é do Sr. Romero Venâncio Rodrigues Filho, que deverá assegurar que tais procedimentos serão realizados na atividade de distribuição das cotas dos fundos de investimento geridos pela Redpoint.

XVI. Erros e Correções

45. Apesar de medidas de prevenção diligentes serem tomadas, erros podem ocorrer e, de fato, ocorrem. Determinados erros de negociação ou operacionais podem potencialmente causar um prejuízo financeiro ou de reputação relevante para a Redpoint e/ou resultar em litígio. A política da Sociedade exige que todos os erros que afetem uma conta de cliente sejam resolvidos de maneira imediata e justa, em consistência com os padrões fiduciários e exigências legais/regulatórias aplicáveis. Para os fins desta política, os erros incluem, entre outros:

(i) Negociações impróprias resultantes de informações incorretas fornecidas ao corretor da negociação; ou

(ii) Negociações/operações inconsistentes com: (a) as diretrizes ou instruções de investimento do cliente; (b) as políticas da Redpoint; e (c) leis e regulamentos aplicáveis.

46. Todos os Membros devem notificar os erros (ou possíveis erros) ao Departamento de Compliance e Gestão de Risco da Redpoint. Os erros devem ser imediatamente investigados, resolvidos e registrados/documentados.

XVII. A Estrutura Interna da Redpoint

47. *Administração.* A Redpoint é administrada por 3 (três) administradores, com anos de experiência em suas áreas de atuação. A administração da Sociedade garante que a Redpoint aja em conformidade com as leis, regulamentos, diretrizes e padrões esperados, incluindo, entre outros:

(i) Realize suas atividades a fim de atingir os objetivos de investimento do(s) titular(es) da carteira;

(ii) Na realização de suas atividades, empregue o cuidado e a diligência que uma pessoa ativa e honesta normalmente empregaria na administração de seu próprio negócio, assumindo a responsabilidade por quaisquer violações ou irregularidades cometidas no curso de sua administração;

(iii) Cumpra, de boa-fé, o acordo prévio por escrito com o cliente, que deve declarar as características básicas dos serviços a serem prestados, incluindo: (a) a política de investimento a ser implementada, que será consistente com o perfil do investidor, sua situação e objetivos financeiros; (b) o pagamento cobrado pelos serviços a serem prestados; (c) as informações com relação a quaisquer outras atividades do Diretor no mercado e possíveis conflitos de interesses que poderão existir entre tais atividades e a administração da carteira de valores mobiliários; (d) os riscos inerentes aos vários tipos de operações com valores mobiliários na bolsa de valores, mercado de balcão, operações de crédito com futuros e ações que ele possa pretender realizar com os recursos fornecidos pelo investidor, declarando, de maneira explícita, que o investimento em derivativos poderá resultar em prejuízos que ultrapassam o investimento feito; (e) autorização, conforme o caso, para o Diretor atuar como contraparte das operações, estabelecido, contudo, que, no caso de um cliente pessoa jurídica, o nome da pessoa física com poderes para conceder tal autorização deve ser declarado por escrito; e (f) o conteúdo e os intervalos de tempo em que o Diretor deve fornecer informações ao cliente;

(iv) Evite práticas que poderão causar danos à relação de confiança com seus clientes;

(v) Atualize e mantenha em perfeito estado e à disposição do cliente todos os documentos relacionados às operações com valores mobiliários incluídos nas carteiras sob sua administração;

(vi) Mantenha em custódia, em uma entidade devidamente qualificada para prestar para tais serviços, os valores mobiliários incluídos nas carteiras sob sua administração, tomando todas as medidas úteis ou necessárias com o objetivo de defender os interesses dos clientes;

(vii) Transfira à carteira quaisquer benefícios ou vantagens que consiga obter por meio de sua capacidade como administrador de carteira; e

(viii) Forneça as informações solicitadas pelo titular da carteira com relação aos valores mobiliários nela incluídos.

48. *Departamento Técnico.* O Departamento Técnico da Sociedade é responsável pela preparação das pesquisas internas de investimentos e das análises de valores mobiliários, as quais irão fundamentar todas as decisões discricionárias de gestão de investimentos tomadas pela ou em nome da Redpoint. Os membros do Departamento Técnico, ainda, serão responsáveis, ainda, pela distribuição das cotas dos fundos geridos pela Redpoint.

49. *Departamento de Compliance e Gestão de Riscos.* É o responsável pela análise do cumprimento dos códigos e políticas da Sociedade, conforme descrito no Capítulo III.

XVIII. Monitoramento das Políticas Atuais

(a) Política de Treinamento

50. Além do treinamento recebido no momento em que cada profissional é admitido na Redpoint, os Membros também participação de uma sessão anual de treinamento, ou sempre que necessário, a respeito dos desenvolvimentos do setor de gestão de carteiras, bem como em relação às políticas implementadas pela Redpoint e quaisquer modificações.

51. As sessões de treinamento serão realizadas pessoalmente, seja em grupo ou individualmente, e serão coordenadas pelo Departamento de Compliance e Gestão de Risco da Redpoint ou por um terceiro contratado para esse fim. As sessões de treinamento abrangerão preferencialmente os seguintes conteúdos: (i) *Fundos de investimento:* regulamentos, tipos de fundos, estratégias de gestão, políticas e objetivos do fundo, prospecto do fundo; (ii) *Compliance e regulamentos:* riscos legais e de imagem, ética, controles internos, segregação de funções e responsabilidades, *chinese wall,* direitos e obrigações de quotistas, divulgação de informações e prestação de contas, procedimentos de investimento e de resgate, conflitos de interesses, entidades regulatórias e supervisoras, auto-regulação; (iii) *Aspectos gerais do mercado financeiro e de capitais*: política monetária, política fiscal, política cambial, indicadores econômicos, taxas de juros, instituições financeiras, entidades reguladoras, mercados primários e secundários, aspectos legais, títulos de dívidas, títulos patrimoniais, instrumentos derivativos; e (iv) *Aspectos técnicos*: desempenho do fundo e indicadores de risco, taxas de gestão e de desempenho, outras taxas, tributação, gestão de risco, riscos de crédito, riscos de mercado, riscos operacionais.

52. Além disso, é necessário que todos os Membros concluam os programas *on-line* sobre ética da Redpoint, promovendo uma cultura fiduciária. Adicionalmente, o treinamento *on-line* da Redpoint sobre combate à corrupção também é obrigatório.

53. O Departamento de Compliance e Gestão de Risco da Redpoint oferecerá outros treinamentos para os Membros. Treinamentos avulsos a respeito de conscientização sobre fraude, segurança da informação, combate à lavagem de dinheiro, canais de denúncia, inclusive ao COAF, e uso seguro de comunicações eletrônicas estão disponíveis e programas adicionais são acrescentados regularmente.

54. O treinamento fornecido aos profissionais da Redpoint deverá focar particularmente nos mecanismos de controle interno, normas de *compliance* e nos deveres e obrigações dos diferentes setores da Sociedade. Todos os profissionais estão devidamente cientes das proibições impostas aos gestores de ativos pelas leis aplicáveis, que incluem: (i) atuar como contraparte, direta ou indiretamente, em operações com carteiras sob sua gestão, exceto nos seguintes casos: (a) quando carteiras individuais estiverem sob gestão e houver consentimento prévio por escrito pelo detentor; ou (b) quando, apesar do gestor ter sido formalmente contratado como gestor da carteira, houver evidência que prove que ele não possui poder discricionário a esse respeito e não possui conhecimento prévio em relação à operação; (ii) fazer qualquer tipo de mudança relevante nas características básicas do serviço prestado, exceto quando houver consentimento prévio por escrito do detentor da carteira; (iii) divulgar quaisquer níveis seguros de lucratividade, com base no histórico de desempenho da carteira ou dos valores mobiliários e das taxas de mercado de capitais; (iv) fazer quaisquer promessas quantificadas em relação a rendimentos futuros da carteira; (v) conceder empréstimos, adiantamentos ou linhas de crédito de qualquer tipo, utilizando recursos sob sua gestão, exceto em caso de empréstimos de ações a terceiros para permitir o desempenho de operações autorizadas pela CVM, estabelecido que haja consentimento prévio por escrito do detentor da carteira; (vi) negociar os valores mobiliários que fazem parte das carteiras sob sua gestão, com a finalidade de gerar receitas de corretagem para si mesmo ou para terceiros; (vii) negligenciar, em qualquer caso, a defesa dos direitos e interesses do detentor da carteira ou ignorar tal defesa; e (viii) promover operações com a finalidade de violar leis tributárias e/ou outras normas legais e regulatórias, mesmo que tais operações melhorem a avaliação da carteira sob gestão.

(b) Política de Segurança

55. O acompanhamento das políticas e procedimentos de segurança e a aplicação de sanções adequadas na hipótese de qualquer infração de tais políticas ou procedimentos serão realizados pelo Departamento de Compliance e Gestão de Risco da Redpoint. Os usuários recebem acesso restrito aos sistemas de informação/tecnologias da Sociedade com um perfil específico, dependendo de suas respectivas tarefas. Uma vez ao ano, os administradores de

domínio (usuários seniores de seus sistemas) deverão, sistema por sistema: (i) conciliar todas as identidades de usuários com os registros do departamento de recursos humanos; (ii) solicitar uma recertificação da lista de usuários; e (iii) manter registros de cada recertificação e das ações de controle realizadas.

56. Independentemente dos mecanismos de controle, sempre que receberem qualquer informação privilegiada, os Membros da Redpoint acordarão, de forma vinculante, em informar imediatamente o Departamento de Compliance e Gestão de Risco da Redpoint (i) caso tal Membro ocupe qualquer cargo no departamento técnico da Redpoint e obteve informação privilegiada de qualquer fonte, inclusive no curso normal de suas atividades; ou (ii) caso esteja trabalhando em uma possível função interna, que recebe regularmente informações privilegiadas, e tenha recebido informações privilegiadas de fontes externas à Sociedade, porém não no curso normal de suas atividades.

57. Com base nas informações recebidas conforme descrito acima, o Departamento de Compliance e Gestão de Risco da Redpoint deverá, uma vez ao mês, criar uma lista contendo as situações de informações privilegiadas que ocorreram no curso do respectivo período. A Redpoint pretende manter permanentemente arquivadas, para consulta futura, todas e quaisquer ocasiões em que seus profissionais informaram a Sociedade sobre possíveis conflitos.

58. De acordo com os dados registrados e de identificação de clientes, para evitar facilitar os crimes de "lavagem de dinheiro" – ou seja, aqueles definidos especificamente nos termos da Lei 9.613 de 3 de março de 1998, conforme alterada pela Lei nº 12.683, de 9.7.2012, e em todos os regulamentos aplicáveis emitidos pela CVM – a Redpoint realizará sessões de treinamento anuais com todos os Membros de forma a evitar a entrada de recursos ilícitos. Ainda no que diz respeito aos dados registrados e de identificação de clientes (a abordagem "*know your client*"), a Sociedade implementará sessões de treinamento anuais para seus Membros a respeito dos procedimentos de registro consistente com as leis aplicáveis. Dentro do escopo da Redpoint, é essencial que todos os Membros estejam cientes dos riscos legais e de imagem na hipótese de qualquer envolvimento direito ou indireto com atividades relacionadas à lavagem de dinheiro. Em caso de dúvidas ou necessidade de orientação, o Departamento de Compliance e Gestão de Risco da Redpoint deverá ser procurado.

59. Adicionalmente, a fim de proteger informações valiosas da Redpoint e evitar sua remoção das instalações da Sociedade, os Membros estão expressamente proibidos de utilizar mídias removíveis (por exemplo, CDs, DVDs, unidades USB e similares) ou meios de comunicação (por exemplo, cabos, rádio, radiação infravermelha e outros) em qualquer computador da Redpoint, exceto se autorizado previamente por escrito, ou por *e-mail* pelo Departamento de Compliance e Gestão de Risco da Redpoint.

60. Além disso, a Redpoint opera uma política de mesa limpa, que exige que determinadas informações em cópia rígida (incluindo discos de computador e CDs) sejam protegidas quando não forem exigidas pelo proprietário/usuário. As exigências da política de mesa limpa são: todas as informações classificadas como Confidenciais e acima devem ser protegidas quando não estiverem em uso: (i) cópia rígida (papel, discos de computadores e CDs etc.) deve ser protegida com cadeado e chave. Grandes volumes de informação devem ser protegidos em áreas de arquivo com acesso permitido àquelas áreas com controle permanente; (ii) telas de computador devem ser posicionadas de forma que os riscos associados com a negligência sejam reduzidos; (iii) sempre que o usuário se afastar do computador de mesa durante o dia de trabalho, o usuário deve se desconectar ou utilizar a proteção de tela. No final do dia de trabalho, o usuário deve desligar o sistema; (iv) mesas, armários para arquivo, armários em geral etc. contendo informações sigilosas devem ser trancados no final do expediente. As chaves desses itens devem ficar em segurança (por exemplo, em armários com chaves); (v) fragmentar documentos confidenciais vencidos ou colocar em fragmentadoras de papel e não utilizar o sistema normal de descarte de lixo; (vi) todos os arquivos "mortos" devem ser arquivados de forma apropriada (ou seja, não devem ser mantidos na estação de trabalho); (vii) todos os itens portáteis de valor devem ser guardados em local seguro, fora do horário comercial. Quando, por questão de trabalho, isso não for possível (por exemplo, o *Notebook* tem de ficar "*on-line*" durante a noite), deve-se tomar medidas para diminuir a atratividade do item para o infrator oportunista (por exemplo, guardar o *notebook* em seu *docking station*).

(c) Política de Negociação Pessoal

61. O acompanhamento das políticas e procedimentos de negociação pessoais e a aplicação de sanções apropriadas, na hipótese de qualquer violação de tais políticas ou procedimentos, deverão ser conduzidos pelo Departamento de Compliance e Gestão de Risco da Redpoint. As seções abaixo detalham as exigências e restrições mínimas de negociação pessoal. Na medida em que a política de negociação pessoal da companhia controladora for mais restritiva, a exigência mais restritiva prevalecerá.

62. Toda conta com uma corretora (conta mantida com uma corretora de valores em que o Membro tem uma participação ou, de outra forma, tem poder direto ou indireto para exercer qualquer tipo de influência sobre as decisões de investimento) deve ser informada e aprovada pelo responsável pelo Departamento de Compliance e Gestão de Risco da Redpoint.

63. O Membro poderá apenas emitir uma ordem de compra ou venda à corretora após obter a autorização do Departamento de Compliance e Gestão de Risco da Redpoint. Tal autorização será concedida levando-se em consideração (i) se o Membro solicitante tem ou possa vir a deter uma participação relevante em uma determinada empresa; e (ii) se o Membro possui qualquer tipo de relacionamento pessoal ou profissional regular com o emissor da empresa em que ele pretende adquirir uma participação acionária. Após obter a

autorização, o Membro terá permissão para emitir a ordem à corretora apenas até o final do dia útil seguinte.

64. O Membro deverá reter as ações por um período mínimo de 14 dias corridos da compra, podendo vendê-las somente após o 15º dia. As exceções a tal prazo poderão ser concedidas apenas pelo Departamento de Compliance e Gestão de Risco da Redpoint. Caso o Membro tenha uma posição ativa em uma conta com uma corretora, o Membro deve necessariamente enviar uma cópia dos extratos mensais de tal conta para o Departamento de Compliance e Gestão de Risco da Redpoint, independentemente de ele ter ou não comprado ou vendido quaisquer ações em tal mês. O Departamento de Compliance e Gestão de Risco da Redpoint poderá lembrar o Membro que o extrato deve ser enviado, porém a responsabilidade pela apresentação do extrato mensal cabe somente ao Membro.

65. As autorizações dadas pelo Departamento de Compliance e Gestão de Risco da Redpoint e as cópias dos extratos mensais referidos neste instrumento deverão ser arquivadas na Sociedade, com a finalidade de verificar qualquer desvio na conduta dos Membros da Redpoint.

(d) Política de Confidencialidade

66. O sucesso da Redpoint depende de sua capacidade de proteger a confidencialidade de suas próprias informações e dos clientes. A Sociedade adotou políticas e procedimentos de barreiras de confidencialidade e informações para: (i) evitar a violação da confidencialidade do cliente; (ii) evitar a violação de proibições legais devido ao uso incorreto de informações privilegiadas relevantes; e (iii) prevenir a percepção do uso incorreto de informações privilegiadas relevantes.

67. A supervisão das políticas e procedimentos definidos nesta Política de Confidencialidade, bem como a execução de sanções, na hipótese de qualquer descumprimento de tais políticas ou procedimentos, deverão ser conduzidas pelo Departamento de Compliance e Gestão de Risco da Redpoint.

68. Os principais meios de restrição do fluxo de informações confidenciais dentro da Redpoint são:

(i) *Com implementação e manutenção de barreiras apropriadas de informações é possível restringir o fluxo de informações confidenciais.* As barreiras de informações são planejadas para restringir o fluxo de informações confidenciais. Isso permite à Redpoint agir adequadamente em relação a terceiros distintos. Para tais finalidades, a Sociedade utiliza *softwares* fornecidos por empresas renomadas, que passam por testes rigorosos de implementação e estão sujeitos a serviços de manutenção regulares. A Política de Segurança descreve práticas adicionais utilizadas no controle dos sistemas da Redpoint.

(ii) *Observação do princípio de "necessidade-de-conhecer".* Apesar de as barreiras de informações serem planejadas para prevenir o fluxo de informações confidenciais, elas não resolverão um possível conflito de interesses se as informações confidenciais tiverem, de fato, atravessado a barreira. Esse é o motivo pelo qual é fundamentalmente importante que os Membros mantenham a confidencialidade das informações privilegiadas em sua posse, compartilhando-as apenas com pessoas que tenham necessidade legítima de delas tomar conhecimento para desempenhar seu trabalho ou concluir uma operação. Os Membros não devem compartilhar informações privilegiadas com nenhuma pessoa dentro ou fora da Redpoint que não tenha uma necessidade legítima de tomar conhecimento das informações. Os Membros não devem divulgar as operações atuais e em curso (a menos que tal divulgação seja necessária para a execução da operação) ou fornecer ou divulgar listas de clientes ou informações de clientes, sem o consentimento do cliente, as concorrentes ou a quaisquer terceiros. A discussão sobre informações confidenciais deve se restringir a áreas privadas. Cuidado similar deve ser tomado em relação à discussão de informações confidenciais de clientes ao usar meios eletrônicos como *e-mail*, bate-papo e *internet*. Todos os Membros devem estar atentos à discussão de questões de clientes no contexto social, mesmo com outros membros da equipe da Sociedade.

(iii) *Observação da Política de Mesa Limpa.* Planejada para proteger a Redpoint contra as consequências de atividade criminal, indiscrição e espionagem industrial. De acordo com a política de Confidencialidade, todos os dados e as informações pessoais e do negócio devem, salvo quando sujeitos a uma isenção de que os dados estão em uma área segura, ser guardados quando os Membros estão ausentes do escritório.

69. A regra mais importante que cada Membro Redpoint deve cumprir é a confidencialidade máxima a respeito de todas as operações do negócio em que a Sociedade está envolvida. Como regra, os profissionais são instruídos a não responder perguntas feitas por pessoas externas que não sejam autoridades relevantes. A Redpoint, como um todo, é responsável pela proteção de seu negócio contra outros e pela confidencialidade de todas as informações de clientes.

70. A norma de confidencialidade aplica-se a informações em todos e quaisquer formatos, sejam decorrentes de conversas, de documentos escritos ou de outra forma. A conscientização da segurança de dados também implica que nenhuma informação com relação à Redpoint será deixada em nenhum local não seguro. Os Membros são instruídos a tomar todas as medidas necessárias para proteger e preservar os documentos ou qualquer objeto de valor em sua posse contra qualquer uso indevido, questionamento impróprio ou exposição indesejada.

71. A Sociedade também se preocupa muito com operações com troca de informações privilegiadas. A troca de informações privilegiadas consiste na negociação de valores

mobiliários de uma companhia aberta com base em informações privilegiadas relevantes (frequentemente denominadas "informações privilegiadas"), a respeito de uma companhia aberta ou de seus valores mobiliários. O ato de divulgar informações privilegiadas a terceiros é normalmente denominado "*tipping*".

72. A capacidade da Redpoint de conduzir suas atividades de gestão de investimento é crítica para o desempenho de suas obrigações fiduciárias perante os clientes. Dessa forma, a adesão a esta Política de Confidencialidade é crítica: uma violação poderá resultar na interrupção de certos serviços de gestão de investimento. Outras consequências legais sérias – para a Sociedade e para o Membro – também poderão resultar de uma violação.

73. Em resumo:

(i) Os Membros não poderão comprar ou vender, ou recomendar a compra ou a venda de valores mobiliários de companhias abertas (incluindo as ações da controladora da Sociedade), pessoalmente ou por meio de clientes, enquanto estiverem de posse de informações privilegiadas relevantes a respeito desses valores mobiliários ou do emissor desses valores mobiliários;

(ii) Os Membros não poderão divulgar informações privilegiadas relevantes a respeito de companhias públicas a outras pessoas, quer dentro ou fora da Redpoint, que não estiverem autorizadas a possuir tais informações; e

(iii) Os Membros não poderão tentar obter informações privilegiadas relevantes que eles não estejam autorizados a possuir. Portanto, exceto se estiverem autorizados, os Membros não devem participar de reuniões em que informações privilegiadas relevantes serão, ou provavelmente serão, discutidas.

74. Os Membros devem notificar o Departamento de Compliance e Gestão de Risco da Redpoint imediatamente caso:

(i) Tenham ou acreditem que uma pessoa possa ter informações privilegiadas a respeito de uma companhia aberta ou de seus valores mobiliários, independentemente de acreditarem que ela está autorizada a possuí-las;

(ii) Saibam ou acreditem que um Membro da Sociedade possa ter quaisquer informações privilegiadas relevantes a respeito de uma companhia aberta ou de seus valores mobiliários que ele não está autorizado a possuir; ou

(iii) Estejam cientes de quaisquer questões envolvendo uso indevido ou possível uso indevido de informações privilegiadas relevantes por outros Membros da Redpoint.

75. Os Membros não devem compartilhar informações privilegiadas com nenhuma outra pessoa que não seja do Departamento de Compliance e Gestão de Risco da Redpoint.

76. A proibição contra a utilização ou a divulgação de informações privilegiadas aplica-se a todos os tipos e classes de valores mobiliários e operações com valores mobiliários. Esta política aplica-se também a operações em créditos corporativos, que poderão não se enquadrar na definição atual de "valores mobiliários". As informações privilegiadas relevantes também poderão se referir a ações do fundo de investimento aberto e fechado.

77. Ao fornecer informações internas em outra posição que não seja a de possível detentor de informações privilegiadas, quando for necessário para a equipe envolvida em uma determinada operação incluir um funcionário da parte pública da operação, por exemplo, um operador ou analista de pesquisa, o Departamento de Compliance e Gestão de Risco da Redpoint deverá informar o funcionário sobre as restrições que se aplicam às suas atividades normais como consequência de tais circunstâncias.

78. Não obstante a necessidade de assegurar a aprovação, por parte do Departamento de Compliance e Gestão de Risco da Redpoint, para permitir que o Membro participe da operação, a aprovação do Departamento de Compliance e Gestão de Risco da Redpoint também será necessária antes de o Membro retomar suas atividades normais, quer envolvam relatórios de operações, de preparação ou de pesquisa ou prospecto de clientes.

79. A Redpoint, por meio do Departamento de Compliance e Gestão de Risco da Redpoint, preparará uma lista de restrições (uma lista das empresas com que a Sociedade considera apropriado restringir operações ou a emissão de relatórios de pesquisa), a ser atualizada conforme necessário. Quaisquer exceções a tais restrições exigirão a aprovação prévia do Departamento de Compliance e Gestão de Risco da Redpoint. O Departamento de Compliance e Gestão de Risco da Redpoint deverá informar quaisquer restrições adicionais, conforme o caso.

80. A Sociedade também deverá criar uma lista de observações (uma lista altamente confidencial de emissores de valores mobiliários com relação aos quais a Redpoint detem informações internas, mas para os quais não foi divulgada publicamente nenhuma operação ou pretensão de operação) permitindo que o Departamento de Compliance e Gestão de Risco da Redpoint monitore as operações e quaisquer pesquisas conduzidas com relação aos valores mobiliários de tais emissores com a finalidade de validar a integridade das barreiras de informações sobre as empresas.

81. A Sociedade está sujeita a exigências amplas de registro. "Manter todas as informações indefinidamente" não é a abordagem correta. Além do custo efetivo de manutenção, há outros

possíveis custos para retenção de documentação que não é necessária:

(i) Todos os registros mantidos pela Redpoint estão sujeitos a certo risco de perda ou roubo, o que poderá prejudicar a Sociedade ou seus clientes;

(ii) Todos os registros mantidos pela Redpoint estão sujeitos a solicitações de órgãos reguladores ou intimação judicial. Em muitos casos, há um custo associado à recuperação e produção de tais registros.

82. É de responsabilidade de todas as unidades de negócio entender e implementar procedimentos adequados para garantir o cumprimento de exigências de retenção de registro em sua unidade e solicitar orientação quando surgirem questionamentos com relação à retenção de registro. Esses procedimentos devem reconhecer o risco de retenção de material desnecessário por períodos mais longos que o exigido. Os Membros devem entender quais registros devem criar e manter e, quando solicitados, devem ser capazes de apresentar tais registros.

83. Para assegurar que a lista de observação funcione efetivamente, a equipe operacional envolvida em atividades que possam estar relacionadas a informações privilegiadas deverá entrar em contato com o Departamento de Compliance e Gestão de Risco da Redpoint, caso (a) a Sociedade tome qualquer iniciativa com relação a um novo acordo e, como consequência de tal ato, recebam informações privilegiadas; e (b) a Redpoint receba informações privilegiadas com relação a recursos de terceiros ou caso ocorram fatos relevantes a respeito de uma operação em andamento.

(e) Métodos gerais de monitoramento

84. Não obstante o acima disposto, a Sociedade e o Departamento de Compliance e Gestão de Risco da Redpoint adotarão os seguintes mecanismos de monitoramento e fiscalização das atividades de seus Membros:

(i) *Antivírus e firewall*. De modo a garantir a integridade dos sistemas e bancos de dados da Redpoint, todos os seus recursos de informática estarão protegidos por sistemas de *firewall*, antivírus e anti-spam, com licenças e softwares constantemente atualizados. Tais recursos monitorarão constantemente os sistemas, para evitar qualquer risco de acesso não autorizado a informações confidenciais.

(ii) *Monitoramento físico*. O prédio no qual se localiza a Sociedade possui portaria de acesso controlado, no qual pessoas trabalhando no edifício possuem cartão individual de acesso, e visitantes são identificados, fotografados e anunciados à empresa que pretendem visitar antes de terem o acesso autorizado, conforme Manual de Gestão de Risco, criando uma barreira

adicional de controle físico de acesso. Igualmente, cada uma das áreas do escritório em que se localiza a Redpoint possui acesso controlado, mediante uso de cartão individualizado e personalizado.

(iii) *Auditoria Interna e Externa*. A Redpoint será submetida às rotinas de auditoria interna de responsabilidade do Departamento de Compliance e Gestão de Risco da Redpoint, o qual aplicará as sanções cabíveis em caso de descumprimento de políticas ou procedimentos adotados pela Sociedade. A Redpoint pode ser submetida às rotinas de auditoria externa de tempos em tempos, ao critério do Departamento de Compliance e Gestão de Risco da Redpoint.

85. Note-se ainda que esta política deve ser lida em conjunto com todas as demais políticas adotadas pela Redpoint.

ANEXO I

Termo de Adesão ao Manual de Compliance

Eu, _____, portador da Cédula de Identidade (RG) nº _____, inscrito(a) no Cadastro de Pessoas Físicas (CPF/MF) sob o nº _____, na qualidade de _____ (cargo) da Redpoint Administradora de Carteiras Ltda., pelo presente instrumento, atesto que:

I – Recebi uma cópia do Manual de Compliance acompanhado da Política de Combate e Prevenção à Lavagem de Dinheiro da Redpoint Administradora de Carteiras Ltda. ("**Manual**");

II. – Recebi treinamento com relação ao seu conteúdo;

III - Tomei ciência dos direitos e obrigações a que estou sujeito; e

IV – Estou de acordo com o inteiro teor do Manual e, como Membro da Redpoint, me responsabilizo pelo descumprimento de qualquer obrigação nela prevista, por ação ou omissão.

Declaro ter lido e aceito integralmente os termos e regras do Manual, expressando total concordância e irrestrita adesão aos referidos termos e regras, sobre os quais declaro não ter dúvidas.

Data:

_____

[Nome do Membro]

* * * * *