INTRADER BLACK STREET CAPITAL

POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

1. INTRODUÇÃO E OBJETIVO 3

1.2. REGULAMENTAÇÃO APLICÁVEL 3

2. DEFINIÇÕES 3

3. CONFIDENCIALIDADE 4

3.1. DIRETRIZES PARA MANUTENÇÃO DA CONFIDENCIALIDADE 4

4. SEGURANÇA DA INFORMAÇÃO 6

4.1. ASPECTOS GERAIS 6
4.2. TESTES PERIÓDICOS 7

5. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA 7

5.1. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS (*RISK ASSESSMENT*) 8
5.2. AÇÕES DE PREVENÇÃO E PROTEÇÃO 8
5.3. PLANO DE RESPOSTA 10
5.4. RECICLAGEM E REVISÃO 10

6. PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS 10

6.1. OBJETIVO 10
6.2. PRINCIPAIS RISCOS POTENCIAIS MAPEADOS 10
6.3. RESPOSTAS DO PCN 11
6.4. MEDIDAS DE PREVENÇÃO 11
6.5. TESTE DE CONTINGÊNCIA 12

7. SEGREGAÇÃO DE ATIVIDADES 12

7.1. ASPECTOS GERAIS 12
7.2. TRATAMENTO DE CONFLITOS DE INTERESSES E SEGREGAÇÃO 12

ANEXO – TERMO DE CONFIDENCIALIDADE 15

1. Introdução e Objetivo

A presente Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética da Gestora tem por objetivo descrever os procedimentos observados pela Gestora para garantir a devida segregação, confidencialidade e segurança das informações e segurança cibernética, para fins de atendimento ao disposto na regulamentação vigente.

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética se aplica a todos os Colaboradores.

1.2. Regulamentação aplicável

- Instrução CVM nº 558/2015, que dispõe sobre o exercício profissional de administração de carteiras de valores;
- Instrução CVM nº 555/2014, que dispõe sobre a constituição, a administração, o funcionamento e a divulgação de informações dos fundos de investimento;
- Instrução CVM nº 356/2001, que regulamenta a constituição e o funcionamento de fundos de investimento em direitos creditórios e de fundos de investimento em cotas de fundos de investimento em direitos creditórios;
- Instrução CVM nº 472/2008, que dispõe sobre a constituição, a administração, o funcionamento, a oferta pública de distribuição de cotas e a divulgação de informações dos Fundos de Investimento Imobiliário;
- Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros;
- Documento de Regras e Procedimentos ANBIMA do Código de Administração de Recursos de Terceiros;

2. Definições

ANBIMA: Associação Brasileira das Entidades do Mercado Financeiro e de Capitais.

Área de *Compliance*: Colaboradores que atuam na área de *compliance* da Gestora.

Área de Gestão: Colaboradores que atuam na área de administração de carteiras de valores mobiliários, na categoria gestor de recursos, da Gestora.

Área de Riscos: Colaboradores que atuam na área de gerenciamento de riscos da Gestora.

B3: Brasil, Bolsa, Balcão.

Colaboradores: todos os colaboradores da Gestora, incluindo sócios, diretores, empregados, consultores, estagiários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Gestora.

Comitê de Risco e *Compliance*: órgão de governança interno da Gestora cujas atribuições, composição e periodicidade das reuniões encontram-se descritas neste documento.

Comitê de Investimentos: órgão de governança interno da Gestora cujas atribuições, composição e periodicidade das reuniões encontram-se descritas, sem se limitar, no formulário de referência Gestora.

CVM: Comissão de Valores Mobiliários.

Diretora de *Compliance* e Risco: diretora estatutária responsável pelas Áreas de *Compliance* e Risco da Gestora.

Diretor de Gestão: diretor estatutário responsável pela atividade de administração de carteiras de valores mobiliários, na categoria gestor de recursos.

Gestora: Intrader Black Street Capital Gestão de Recursos Ltda.

Política de Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética: o presente documento.

Veículo(s) de Investimento(s): fundos de investimento e carteiras administradas sob gestão da Gestora.

3. Confidencialidade

3.1. Diretrizes para Manutenção da Confidencialidade

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Gestora são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na Gestora e sempre em benefício dos interesses desta e de seus clientes.

A utilização de informação privilegiada para obter vantagens, mesmo que pelos Colaboradores envolvidos na circunstância, é considerada ato ilícito.

São exemplos de informações privilegiadas:

- Informações verbais ou documentadas a respeito de resultados operacionais de empresas;
- Alterações societárias (fusões, cisões e incorporações);
- Informações sobre compra e venda de empresas;
- Títulos ou valores mobiliários, e;
- Qualquer outra informação que seja objeto de um acordo de confidencialidade firmado pela Gestora com terceiros.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes da Gestora deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, por escrito, salvo na hipótese de decisão judicial específica que determine à Gestora a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da CVM. Caso a Gestora ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser comunicado aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os Colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais, e manter sigilo sobre senhas do computador, rede e sistemas. Os colaboradores devem garantir que o acesso à área de trabalho seja feito somente por pessoal autorizado.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Gestora, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Gestora. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da Gestora, para que sejam tomadas as medidas cabíveis.

A Gestora exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Gestora, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

O material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Gestora, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa, por escrito, da Diretora de *Compliance* e Risco. Ainda, os arquivos eletrônicos recebidos ou gerados pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo da área, do cliente ou do projeto a que se refere tal arquivo eletrônico.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade da Gestora, presente no anexo à presente Política, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Gestora e durante certo período após terem deixado a Gestora.

Neste sentido, os Colaboradores, no término de sua relação com a Gestora, devolverão todos os originais e todas as cópias de quaisquer informações recebidas ou adquiridas, bem como todos os arquivos, correspondências e/ou outras comunicações recebidas, mantidas e/ou elaboradas durante o respectivo contrato.

Para fins de manutenção das informações confidenciais, a Gestora recomenda que seus Colaboradores (i) bloqueiem o computador quando o mesmo não tiver sendo utilizado ou estiverem ausentes da sua estação de trabalho; (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartem materiais usados, destruindo-os fisicamente e (iv) jamais revelem a senha pessoal de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

3.2. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora (“Informações” ou “Informação”), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, a Diretora de *Compliance* e Risco deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, a Diretora de *Compliance* e Risco, primeiramente, identificará se a Informação vazada refere-se ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, a Diretora de *Compliance* e Risco procederá da seguinte forma:

No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

No caso de vazamento de Informações relativas aos cotistas:

Neste caso, a Diretora de *Compliance* e Risco procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, a Diretora de *Compliance* e Risco ficará à inteira disposição para auxiliar na solução da questão.

4. Segurança da Informação

4.1. Aspectos Gerais

São considerados como parte dos sistemas de informação os equipamentos, programas, dados e informações assim como telefones e aparelhos para conferências. Desta forma, em síntese, visando preservar a segurança das informações, a Gestora adota os seguintes procedimentos:

- Todos os sistemas de informação são voltados exclusivamente para realização das atividades que o Colaborador é designado. Todo Colaborador que tiver acesso aos sistemas de informação da Gestora é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas;

- A cópia de informações depende de autorização expressa e prévia da área responsável e deve observar os direitos de propriedade intelectual;

- Todos os dados transitados pelos sistemas são passíveis de auditoria;

- As informações geradas e administradas voltadas à atividade de gestão de recursos de terceiros são restritas aos profissionais da Área de Gestão, sem prejuízo da possibilidade de a Diretora de *Compliance* e Risco acessa-las com o estrito objetivo de desenvolver as suas atividades, de modo que há segregação absoluta dos arquivos e informações confidenciais correspondentes. Os Colaboradores integrantes da Área de Gestão atuarão exclusivamente na Gestora, e não se envolverão quaisquer atividades operacionais desempenhadas pelas demais áreas da Gestora ou outras empresas integrantes do grupo econômico da Gestora;

- As informações que os Colaboradores venham ter acesso em razão do exercício de suas funções não poderão ser transferidas a pessoas não autorizadas ou que possam utilizá-las de forma indevida;

- O acesso aos sistemas de informação da Gestora é feito por meio de um par “usuário/senha”. O acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Gestora. O controle desses dados é de domínio da Gestora, uma vez que o armazenamento dos dados

ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação;

- Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros ou compartilhadas. As senhas são de caráter sigiloso, pessoal e intransferível e serão fornecidas aos Colaboradores da Gestora para acesso às estações de trabalho, à rede corporativa e ao correio eletrônico corporativo;

- O responsável pela rede corporativa será o único autorizado a atribuir senhas de acesso. Os logins à rede identificarão claramente seu detentor, na forma como ele é reconhecido na Gestora através da representação de seu nome. O controle de acesso à rede será atribuído conforme o perfil do usuário;

- Sempre que o Colaborador se ausentar de sua estação de trabalho deverá efetuar o bloqueio de sua máquina;

- Visitantes nunca deverão estar desacompanhados e não poderão adentrar no espaço destinado à Área de Gestão;

- Somente Colaboradores autorizados poderão circular nas dependências da Gestora;

- Ao final da sua rotina de trabalho, os Colaboradores deverão recolher todo o material impresso que contenha informação sensível;

- Todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas fisicamente na sede da Gestora, com *backup* de dados, na nuvem, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência; e

- Todos os acessos concedidos pela Gestora são imediatamente cancelados em caso de desligamento do Colaborador.

4.2. Testes Periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Verificação semestral do login dos Colaboradores;
(ii) Anualmente, altera-se a senha de acesso dos Colaboradores;
(iii) Testes trimestrais no firewall;
(iv) Testes semestrais nas restrições impostas aos diretórios;
(v) Manutenção semestral de todo o “hardware” por empresa especializada em consultoria de tecnologia de informação;
(vi) Testes no *backup* (salvamento de informações) semanal, realizado na nuvem.

5. Procedimentos de Segurança Cibernética

Responsável: Diretora de *Compliance* e Risco

5.1. Identificação e avaliação de riscos (*risk assessment*)

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. Os ataques mais comuns de *cybercriminals* são os seguintes:

(i) Malware (vírus, cavalo de troia, spyware e ransomware);
(ii) Engenharia Social;
(iii) Pharming;
(iv) Phishing scam;
(v) Vishing;
(vi) Smishing;
(vii) Acesso pessoal;
(viii) Ataques de DDoS e botnets;
(ix) Invasões (advanced persistent threats).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Gestora definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A Gestora levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

5.2. Ações de prevenção e proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a Gestora adota, conforme já detalhado nas regras internas que tratam de Segurança da Informação e Segregação de Atividades.

A Gestora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis. A Gestora deve criar logs e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela Segurança Cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A Gestora conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais. A Gestora deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pela Diretora de *Compliance* e Risco.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da

Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

A utilização dos sistemas de informação da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

Todos os anexos dos e-mails recebidos pelos Colaboradores da Gestora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

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

A Gestora adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da Gestora.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 16 da Instrução CVM nº 558/15, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da Gestora e devem ser observadas integralmente.

A Gestora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A Gestora mantém inventários atualizados de hardware e software, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da Gestora deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A área responsável deve também monitorar diariamente as rotinas de *backup*, executando testes regulares de restauração dos dados.

Deve-se, ademais, realizar testes de invasão externa, phishing, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados na forma definida no item anterior devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

5.3. Plano de resposta

A Área de *Compliance* deve, conjuntamente com os profissionais de *cybersecurity* e segurança da informação, elaborar um plano formal de resposta a ataques virtuais. A Gestora deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deverá levar em conta os cenários de ameaças previstos no *risk assessment*. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

5.4. Reciclagem e revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da Gestora sobre a matéria, deverá ser revisto e atualizado semestralmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A Gestora deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

6. Plano de Contingência e Continuidade dos Negócios

6.1. Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal em suas instalações principais, a Gestora possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada Colaborador na execução do Plano de Continuidade de Negócio (“PCN”).

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela Gestora, de forma que os interesses dos clientes da Gestora não sejam prejudicados.

O PCN estabelecido e sua ativação é responsabilidade da Diretora de *Compliance* e Risco. Periodicamente, o plano será revisado pela Diretora de *Compliance* e Risco com a finalidade de: (i) verificar que o PCN esteja em concordância com as leis e normas dos órgãos reguladores e (ii) zelar por sua atualização e cumprimento do cronograma de treinamento previsto.

6.2. Principais riscos potenciais mapeados

A análise do impacto do negócio foi resumida para refletir os potenciais riscos que podem causar desastres, incidentes e consequentes possíveis perdas ao negócio da Gestora. São eles:

1. Queda de energia.

No-break para até 1 (uma) hora.

2. Queda do link para acesso à internet.

Links redundantes de operadoras diferentes e utilização de modens de operadoras de Celular.

Caso nenhuma das contingências funcionem, é possível fazer o acesso remoto aos e-mails, que podem ser acessados através de outros provedores.

3. Contingências para e-mail e rede de arquivos.

Indisponibilidade do serviço de e-mail e rede de arquivos.

4. Invasão da intranet por hackers.

Firewall com monitoramento e alertas de segurança.

5. Impossibilidade de acessar o escritório

Algum desastre ou outro fato de força maior impede os funcionários de acessarem o escritório.

6.3. Respostas do PCN

Para os pontos “1” e “2”, a Gestora entende que a solução mais rápida é a utilização de outro computador de fora do escritório com acesso à internet.

Para o item “3”, o serviço de e-mail é poderá ser acessado remotamente, garantindo a continuidade. Há possibilidade de comunicação nos celulares dos Colaboradores.

No item “4” e “5” o recomendado é utilizar a estação em nuvem, que possui acesso direto ao *backup* dos arquivos.

A implementação dos planos de contingência deverá ser realizada em até quatro horas e será de responsabilidade da Diretora de *Compliance* e Risco.

O reestabelecimento da operação poderá ser realizado por terceiros contratados e o prazo de ajuste será estimado pelo prestador de serviço em questão.

Adicionalmente, se necessário, a Gestora adotará soluções para:

(i) Substituir equipamentos danificados;
(ii) Efetuar despesas contingenciais, incluindo a compra de equipamentos ou contratação de serviços que se fizerem necessários;
(iii) Avaliar os prejuízos decorrentes da interrupção das atividades regulares.

6.4. Medidas de Prevenção

A Gestora realiza o *backup* de seus dados diariamente, possibilitando o acesso às últimas versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Os principais executivos da Gestora possuem acesso remoto aos seus e-mails, de modo que possam acessá-los de fora do escritório, se necessário.

Os registros contábeis da Gestora ficarão com o contador responsável (terceirizado) e as informações sobre os fundos de investimento cujas carteiras serão geridas pela empresa ficarão com a respectiva instituição administradora.

A equipe de gestão da Gestora tem acesso a softwares que permitem a consulta do mercado financeiro em qualquer lugar do mundo.

6.5. Teste de Contingência

Será planejada a realização de testes de contingências anualmente, sob responsabilidade da Diretora de *Compliance* e Risco, sem prejuízo da implementação de testes que se façam necessários em uma menor periodicidade, de modo a possibilitar que a Gestora esteja preparada para a continuação de suas atividades. Tais testes devem ser realizados com o objetivo de verificar as condições para:

(i) Acesso aos sistemas;
(ii) Acesso ao e-mail corporativo;
(iii) Acesso aos dados armazenados em procedimento de *backup*; e
(iv) Outros necessários à continuidade das atividades da Gestora.

O resultado de cada teste anual será registrado em relatório próprio obedecendo o disposto na regulamentação aplicável e as orientações das entidades responsáveis pela supervisão das atividades, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do presente PCN.

O PCN foi elaborado tendo em vista a possibilidade de realização de todos os trabalhos prestados pela Gestora sem dependência do acesso à sua localidade física.

7. Segregação de Atividades

7.1. Aspectos Gerais

A Intrader Black Street Capital Gestão de Recursos Ltda é uma gestora de investimentos independente com autorização de funcionamento em conformidade com a Instrução CVM nº 558/2015.

Visando atribuir o mais elevado grau de transparência, salienta-se que a Gestora possui como sócia controladora direta a pessoa jurídica Intrader Holding Não Financeira Ltda. (“Intrader Holding”), sociedade que não exerce atividades de cunho operacional, e não exerce o controle de outras instituições além da Intrader DTVM, adiante definida, que representam situações de conflitos de interesses com a Gestora. A Intrader Holding, por sua vez, é controlada por sócio pessoa física que também exerce controle da Intrader Distribuidora de Títulos e Valores Mobiliários Ltda., inscrita no CNPJ/ME sob o n° 15.489.568/0001-95 (“Intrader DTVM”), sendo a Intrader DTVM, portanto, empresa sob controle comum. Inclusive, a Intrader DTVM possui uma participação minoritária na Gestora. A Intrader DTVM atua como uma distribuidora de títulos e valores, sendo habilitada perante a CVM e o Banco Central do Brasil para o exercício das suas atividades, que inclui a administração fiduciária de fundos de investimentos, escrituração e custódia de ativos financeiros.

7.2. Tratamento de conflitos de interesses e Segregação

A Intrader Holding não exerce atividades de cunho operacional, não havendo que se falar, portanto, em conflitos de interesse com a Gestora.

Não obstante, ciente da existência de conflitos de interesses entre a Gestora e a Intrader DTVM, a Gestora adota as seguintes práticas centrais para eliminar ou mitigar eventuais conflitos, potenciais ou existentes:

I. Segregação Física:

A Gestora e a Intrader DTVM são segregadas fisicamente, de modo que os espaços de cada uma das empresas são fechados e possuem controles de acesso eletrônicos. Ademais, cumpre salientar que o espaço destinado à área de gestão é restrito aos colaboradores da área de gestão –

observada a possibilidade de acesso do diretor responsável pelas áreas de compliance, risco e PLDFT para estrito cumprimento das suas tarefas.

II. Segregação Lógica:

Existe a segregação lógica entre a Gestora e a Intrader DTVM, sendo os acessos aos diretórios completamente segregados, com controle individual de acesso, de forma a garantir o máximo nível de confidencialidade das informações e manter o sigilo devido das operações realizadas pela Gestora, conforme especificado na presente política.

III. Segregação Funcional:

Os Colaboradores integrantes da Área de Gestão da Gestora atuarão exclusivamente na consecução das atividades inerentes à referida área, de modo que tais profissionais não desempenharão qualquer função operacional na Intrader DTVM. Inclusive, tais Colaboradores não terão qualquer acesso às informações relativas às atividades operacionais da Intrader DTVM. A mesma regra se aplica aos profissionais das áreas de administração fiduciária de fundos de investimentos, escrituração e custódia de ativos financeiros da Intrader DTVM (i.e., tais profissionais não atuarão, de qualquer forma, na Gestora).

Desta forma, visando a mitigação de cenários de conflitos de interesses, a Gestora e a Intrader DTVM mantêm suas estruturas segregadas, compartilhando somente as diretorias de *compliance*, risco e PLDFT, conforme faculdade prevista no artigo 4°, §4°, da Instrução CVM nº 558/2015, além de poder alocar pessoal da Intrader DTVM para prestar serviços de suporte como *operations*, jurídico, financeiro e administrativo. Ademais, o sócio executivo da Intrader DTVM, o Sr. Edson Hydalgo Júnior, atuará como Diretor de Gestão.

IV. *Disclousure*:

A Gestora sempre dará *disclousure* aos seus clientes acerca da existência da Intrader DTVM em seu grupo econômico, sendo certo que operações com partes relacionadas observarão integralmente o disposto na regulamentação vigente aplicável para o veículo de investimento sob gestão da Gestora que pretender realizar tal operação.

Sem prejuízo, cumpre salientar, ainda, que para salvaguardar eventuais conflitos de interesse, todo e qualquer benefício recebido pela Gestora diretamente ou indiretamente, serão integralmente revertidos aos seus clientes, conforme estabelecido na regulamentação em vigor. Ademais, eventuais rebates recebidos por investimentos feitos pelos veículos de investimento geridos pela Gestora serão devolvidos aos próprios veículos de investimento, exceto nos casos de investimentos feitos por (a) investidores profissionais que tenham assinado o Termo de Ciência previsto na Instrução CVM nº 555/2014, ou (b) fundo de investimento em cotas de fundo de investimento que invista mais de 95% (noventa e cinco por cento) de seu patrimônio em um único fundo de investimento.

Não obstante, a Gestora atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito de interesses entre atividades prestadas pela Gestora. Não obstante, a Gestora manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

Ademais, a Gestora adota segregação interna. O primeiro nível de segregação dentro das atividades da Gestora refere-se às diferenças funcionais de atuação e autoridades definidas para

as posições de gestor, analistas, *compliance*, risco e administrativo. Perfis de acesso, e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade (“as-needed basis”) nos comitês instituídos pela Gestora, sendo que os participantes se responsabilizam pelo sigilo das informações.

As diferentes áreas da Gestora terão suas estruturas de armazenamento de informações logicamente segregadas das demais, de modo a garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

Sem prejuízo, as regras destacadas na política de Segurança da Informação, tratada neste documento, sobretudo no que tange às segregações eletrônicas e de funções, se aplicam para fins da presente política de Segregação das Atividades, e devem ser observadas pelos Colaboradores da Gestora.

ANEXO – TERMO DE CONFIDENCIALIDADE

Através deste instrumento, _____, inscrito no CPF sob o no _____, doravante denominado Colaborador, e Intrader Black Street Capital Gestão de Recursos Ltda. (“Gestora”), resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade (“Termo”), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais (“Informações Confidenciais”), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, que não sejam de domínio público, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes, independente destas informações estarem contidas em discos, pen-drives, fitas, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Gestora, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, que não sejam de domínio público.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar informações privilegiadas, *insider trading*, Divulgação Privilegiada e front running, seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2 A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Gestora e terceiros, ficando

desde já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, ou desligamento ou exclusão por justa causa, conforme a função do Colaborador à época do fato, obrigando-lhe a indenizar a Gestora e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.

3.2 O Colaborador expressamente autoriza a Gestora a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos, observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízos do direito do Gestora de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

3.3 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

3.4 O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;
b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;
c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos (“Informação Protegida”), são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à

base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei;
d) Nos termos da Lei 9.279/95, é proibida a divulgação, exploração ou utilização sem autorização, de Informação Protegida a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese de o Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1 Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

5.2 A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Cidade], [data]

_____

[COLABORADOR]