m square

Manual De *Compliance*

Regras, Procedimentos
e Descrição dos Controles Internos

Este Manual de *Compliance* é de propriedade
da M Square Investimentos LTDA. e deve ser devolvido
à gestora caso o vínculo do colaborador termine por qualquer motivo.
O conteúdo deste manual é confidencial e não deve ser
Revelado a terceiros sem o consentimento do(a) Diretor(a) de *Compliance*.

M Square Investimentos LTDA.
Junho de 2022

m square

Índice

1 INTRODUÇÃO 5

1.1 Finalidade 5

1.1.1 Segregação de Atividades - Independência 6

1.2 Uso do Manual 6

1.3 Sanções 8

1.4 Aditamentos 8

1.5 Questões 9

2 OBRIGAÇÕES FIDUCIÁRIAS 9

2.1 Princípios Fiduciários Gerais 9

2.2 Lei Anticorrupção Brasileira (Lei 12.846/13) e Decreto Regulamentar (8.420/2015) 10

2.3 Procedimentos Operacionais e Revisão de *Compliance* 13

3 CONFLITOS DE INTERESSES 13

3.1 Introdução 13

3.2 Identificando Conflitos de Interesses 14

3.2.1 Conflitos entre a Gestora e seus Veículos de Investimento 14

3.2.2 Conflitos entre Colaboradores e os Veículos de Investimento 14

3.2.3 Conflitos entre os Veículos de Investimento 14

3.2.4 Conflitos entre Investidores 14

3.2.5 Conflitos com Atividades e Negócios Externos 14

3.3 Procedimentos Operacionais e Revisão de *Compliance* 15

4 OFERTAS E *SUITABILITY* DO INVESTIDOR 15

4.1 Regulamentações de *Suitability* no Brasil 15

4.2 Procedimentos Operacionais e Revisão de *Compliance* 16

5 MANUTENÇÃO DE LIVROS E REGISTROS 16

5.1 Introdução 16

5.2 Registros Típicos de Atividades 17

5.3 Registros Adicionais 17

5.4 Períodos de Arquivamento 17

5.5 Registros Eletrônicos 18

m square

5.6 Procedimentos Operacionais e Revisão de *Compliance* 18

6 PROPAGANDA E MARKETING 18

6.1 Introdução 18

6.2 Propaganda e Marketing no Brasil 18

6.3 Política de Materiais de Propaganda e Marketing 20

6.3.1 Diretrizes Gerais 20

6.3.2 São exemplos de Material Publicitário e Material Técnico 21

6.3.3 Não são considerados Material Publicitário ou Material Técnico: 21

6.3.4 Processo de aprovação de Materiais Publicitários ou Materiais Técnicos 22

6.3.5 Solicitação de aprovação de Material ou Material Técnico 23

6.3.6 Diretrizes para confecção e distribuição de Material Publicitário ou Material Técnico 23

6.3.7 Diretrizes para confecção de Qualificações 25

6.3.8 Diretrizes para Comparação e Simulação, Histórico de Rentabilidade, Avisos Obrigatórios e Selos 25

7 COMUNICAÇÕES COM O PÚBLICO 26

7.1 Políticas de Comunicações com o Público 26

7.1.1 Meios de Comunicação 26

7.1.2 Salas de *Chat* 27

7.1.3 Mídia Social 27

7.1.4 Participação em Conferências 27

7.2 Procedimentos Operacionais e Revisão de *Compliance* 27

8 OPERAÇÕES E MELHOR EXECUÇÃO 28

8.1 Introdução 28

8.2 *Soft Dollars* 28

8.3.1 Lista de Contrapartes Aprovadas 29

8.3.2 Revisão de Contrapartes 30

8.3.3 Procedimentos Operacionais e Revisão de *Compliance* para Melhor Execução 30

8.4 Registro de Ordens de Operação 30

8.5 Erros Operacionais 30

8.5.1 Política de Erros Operacionais 30

8.5.2 Procedimentos Operacionais e Revisão de *Compliance* para Erros Operacionais 31

m square

9 RECLAMAÇÕES 31

9.1 Introdução 31

9.2 Definição 31

9.3 Lidando com Reclamações 32

9.3.1 Responsabilidade de Colaboradores 32

9.3.2 Revisão pela Diretor(a) de *Compliance* 32

9.3.3 Procedimentos Operacionais e Revisão de *Compliance* 32

10 POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO 32

10.1 Introdução 32

10.2 Aviso de Política de Confidencialidade 33

10.3 Divulgação das Informações Pessoais Não Públicas 33

10.4 Controles de Acesso 34

10.5 Proteção à Base de Dados 35

10.6 Identificação dos detentores da informação, manutenção de registros e logs 36

10.7 Vazamento de Informações Confidenciais 36

10.8 Treinamento, Testes de Segurança e Revisão de *Compliance* 37

11 FATCA 37

11.1 Introdução 37

11.2 Política de FATCA 38

11.3 Procedimentos Operacionais e Revisão 38

11.4 Designação de Diretora Responsável 39

12 PLANO DE CONTINGÊNCIA E RECUPERAÇÃO DE DESASTRE 39

12.1 Plano 39

12.2 Treinamento 39

12.3 Teste 39

12.4 Procedimentos Operacionais e Revisão de *Compliance* 40

ANEXO I 41

ANEXO II 55

ANEXO III 72

ANEXO IV 75

ANEXO V 79

ANEXO VII 87

ANEXO VIII 87

ANEXO IX 104

ANEXO X ..... ERROR! BOOKMARK NOT DEFINED.

1. Introdução

Este Manual de *Compliance* (o "**Manual**") foi desenvolvido para auxiliar todos os parceiros, sócios, diretores, empregados (permanentes ou temporários), estagiários (coletivamente, "**Colaboradores**"), consultores e outras pessoas que em razão de sua posição, relação societária ou comercial com a M Square Investimentos Ltda. ("**M Square**" ou a "**Gestora**"), ou ainda que regularmente estejam presentes nos escritórios da M Square (cada um individualmente **"Representante"**), a cumprirem com as disposições aplicáveis da Lei nº 6.385 de 1976 que dispõe sobre o Mercado de Valores Mobiliários, conforme alterada e outras leis e regulamentações aplicáveis vigentes no Brasil (coletivamente, "**Lei Aplicável**"), incluindo as normas adotadas pela, Comissão de Valores Mobiliários do Brasil ("**CVM**") e Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("**ANBIMA**").

Os Colaboradores também devem consultar o Código de Ética ("**Código de Ética**"), bem como as demais políticas constantes do presente Manual, para informações adicionais sobre as políticas e procedimentos da M Square pertinentes ao tratamento de informação privilegiada, política de compra e venda de valores mobiliários por administradores, empregados e pela própria Gestora, e a gestão de eventuais conflitos de interesse, e o Plano de Contingência da Gestora, disponível no website da Gestora (www.msquare.com.br) para informações sobre os procedimentos adequados em cenários de contingência ou desastre.

1.1 Finalidade

A CVM pode utilizar o termo cliente para representar o investidor final. Para os fins deste Manual, os veículos e investidores da M Square seguem abaixo definidos.

A M Square é atualmente uma gestora com poder discricionário de investimento para fundos brasileiros registrados na CVM (os "**Fundos CVM**") e Fundos de Fundos Internacionais (os "**Fundos *Offshore***"), todos coletivamente, doravante denominados como "**Veículos de Investimento**".

O Manual tem como base o princípio de que cada Colaborador e eventual Representante tem um dever fiduciário para com os Veículos de Investimento, bem como para com aqueles que investem nos Veículos de Investimento (os "**Investidores**").

No Brasil, a M Square é autorizada a atuar como administradora de carteira de valores mobiliários, na categoria gestor de recursos, de acordo com a Instrução CVM 558 de 2015, de 26 de março de 2015, conforme alterada ("**Instrução CVM 558**"). Além do mais, embora autorizada, atualmente a M Square

não gere carteiras administradas para Investidores no Brasil, e atua somente como administradora de carteira de valores mobiliários para os Fundos CVM.

À luz desse dever fiduciário, a Gestora exige que os Colaboradores:

- Coloquem os interesses dos Veículos de Investimento e Investidores à frente de seus próprios interesses a todo o tempo;
- Conduzam suas operações (incluindo pessoais) de acordo com este Manual, o Código de Ética e a Política de Investimentos Pessoais, de forma a evitar qualquer conflito de interesse efetivo ou potencial;
- Sigam o princípio de que gestores de recursos de terceiros não devem obter benefícios pessoais indevidos em decorrência de sua posição; e
- Representem a Gestora e cumpram seu papel dentro dela corretamente.

Assim, o principal objetivo do presente Manual constitui a consolidação das regras, procedimentos e descrição dos controles internos adotados pela Gestora (incluindo, mas sem limitação, aqueles demandados pela Instrução CVM 558). Adicionalmente, o presente Manual abrange outras práticas e políticas adotadas pela Gestora, tais como a política de rateio e divisão de ordens entre os Veículos de Investimento sob sua gestão e a política de prevenção e combate à lavagem de dinheiro, dentre outras.

1.1.1 Segregação de Atividades - Independência

A M Square somente exerce atividade de gestão de recursos de carteiras de valores mobiliários de terceiros. Assim sendo, não se aplicam à M Square as regras referentes à segregação de atividades exigidas pela regulamentação aplicável, uma vez que não há a possibilidade de configuração de conflito de interesses nesta hipótese.

Entretanto, a M Square possui participação societária em outra sociedade, cujo(s) sócio(s) pode(m) trabalhar fisicamente em escritórios da M Square. Nesse sentido, a M Square desenvolveu a Política de Segregação de Atividades e Prevenção de Conflitos de Interesses (Anexo IV deste Manual), de forma a prevenir conflitos decorrentes da utilização de parte do espaço físico por terceiros que não sejam Colaboradores da M Square.

1.2 Uso do Manual

Cada Colaborador deve:

- Manter uma cópia, se familiarizar e entender o conteúdo deste Manual, bem como do Código de Ética, e assegurar a observância de seu conteúdo em suas atividades diárias;
- Completar, assinar, declarar ciência e devolver a(o) Diretor(a) de *Compliance*, dentro de 10 (dez) dias a partir do início do vínculo empregatício com a M Square:
    - O "**Comprovante de Recebimento e Compromisso de Cumprimento**" anexado ao Código de Ética sob a forma do Anexo I;
    - O "**Instrumento de Política Comercial**" anexado ao Código de Ética sob a forma de Anexo VI;
    - O "**Compromisso de Responsabilidade e Confidencialidade**" anexado ao Código de Ética sob a forma de Anexo VII;
    - O "**Relatório de Investimentos Reportáveis**" anexado ao Código de Ética sob a forma do Anexo IV;
    - A "**Declaração de Atividade Externa / Posição de Insider**" anexado ao Código de Ética sob a forma do Anexo II;
    - O "**Atestado de Antecedentes**" anexado ao Código de Ética I sob a forma de Anexo VIII, o qual deverá ser atualizado e enviado a(o) Diretor(a) de Risco e *Compliance* sempre que houver alterações na situação do Colaborador.
- Obter autorização prévia para realizar Investimentos Privados acima do percentual de 25% (vinte e cinco por cento) da sociedade, veículo de investimento, empreendimento ou emissão privada, conforme definido no Código de Ética da M Square, através do "**Formulário de Pré-Autorização para Investimentos Privados**" na forma do Anexo V do Código de Ética, ou negociar determinados ativos que necessitem de aprovação do(a) Diretor(a) de Risco e *Compliance*, de acordo com o item 6.3 e seus subitens da Política de Investimentos Pessoais, devendo enviar tal solicitação através do e-mail *Compliance*@msquare.com.br;
- Comunicar previamente a(o) Diretor(a) de Risco e *Compliance*, através da Declaração de Atividade Externa / Posição de Insider, na forma do Anexo II do Código de Ética, caso o Colaborador pretenda realizar Atividades Externas, conforme definido no item 3.3 do Código de Ética da M Square;
- No caso de sócios controladores diretos e indiretos, e diretores da M Square, estes devem comunicar prontamente ao *Compliance*, através do e-mail *Compliance*@msquare.com.br, acerca de processos judiciais ou administrativos instaurados contra si, e questões

midiáticas negativas o envolvendo (ex. envolvimento em atos de corrupção, esquemas de lavagem de dinheiro, etc.).

1.3 Sanções

As sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual serão definidas pelo Comitê de Risco e *Compliance,* a seu exclusivo critério, garantido, contudo, ao Colaborador suspeito, o direito de defesa. Poderão ser aplicadas, entre outras, penas de advertência, suspensão, desligamento ou demissão por justa causa, nesse último caso, nos termos do artigo 482 da Consolidação das Leis de Trabalho – CLT, sem prejuízos do direito da M Square de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio de medidas legais cabíveis.

A utilização da esfera disciplinar interna não visa limitar a efetivação de medidas legais cabíveis para reparar qualquer dano provocado à M Square, seus clientes ou Investidores, os quais poderão tomar as medidas cabíveis para eventual ressarcimento inclusive pecuniário, se for o caso.

Se ocorrer uma violação deste Manual ou do Código de Ética, além das ações cabíveis acima, o(a) Diretor(a) de Risco e *Compliance* também poderá exigir que o Colaborador infrator reverta a operação em questão, renuncie qualquer lucro, e/ou absorva qualquer prejuízo decorrente da operação. A Gestora se reserva o direito único e absoluto de determinar a sanção a ser imposta sobre qualquer Colaborador. Cada Colaborador deve atentar aos princípios gerais, finalidades e espírito deste Manual, além das políticas e procedimentos específicos.

Qualquer Colaborador da M Square que tome conhecimento de informações ou circunstâncias que possam afetar os interesses da M Square ou criar um conflito ou que possa ser contrário aos termos deste Manual, notificará seu superior imediato, o(a) Diretor(a) de Risco e *Compliance* ou qualquer membro do Comitê de Risco e *Compliance*, de modo que o Comitê de Risco e *Compliance* possa determinar as medidas adequadas a serem tomadas.

Por outro lado, se o(a) Diretor(a) de Risco e *Compliance* violar as disposições deste Manual, do Código de Ética ou demais políticas, os demais integrantes do Comitê de Risco e *Compliance* da M Square determinarão, de forma colegiada, as medidas disciplinares cabíveis.

1.4 Aditamentos

A Gestora aditará este Manual, conforme necessário, quando ocorrerem alterações das Leis Aplicáveis, e conforme ocorram alterações nas atividades da Gestora, suas políticas ou procedimentos. Quaisquer alterações relevantes serão comunicadas aos Colaboradores.

1.5 Questões

Se um Colaborador tiver uma dúvida referente a este Manual, deve consultar o(a) Diretor(a) de Risco e *Compliance*.

2. Obrigações Fiduciárias

2.1 Princípios Fiduciários Gerais

Pela natureza de sua relação com os Veículos de Investimento, a Gestora é considerada uma fiduciária.

Alguns dos princípios fiduciários gerais aplicáveis à Gestora estão listados a seguir.

- ***Gestão sem Conflito de Interesse*** – a Gestora deve fornecer orientações de gestão das carteiras dos Veículos de Investimento que sejam adequadas aos seus Veículos de Investimento e Investidores, no melhor interesse dos mesmos.
- ***Divulgação dos Conflitos de Interesse*** – Em todos os documentos relacionados aos Veículos de Investimento, a Gestora deve detalhar por escrito todas as hipóteses em que poderão surgir conflitos de interesses concorrentes à prestação dos serviços de gestão.
- ***Confidencialidade*** – Os registros e informações financeiras de cada Investidor devem ser tratados com estrita confidencialidade. Sob nenhuma circunstância, qualquer informação confidencial será divulgada a um terceiro não autorizado pelos Investidores a receber tais informações (vide Seção 11 – Política de Confidencialidade e Segurança da Informação).
- ***Fraude*** – a Gestora não empregará qualquer dispositivo, esquema ou artifício para fraudar os Veículos de Investimento, Investidores, clientes ou Investidores potenciais; tampouco engajar-se-á em qualquer operação, prática ou atividade que fraude os Veículos de Investimento, Investidores, clientes ou Investidores potenciais.

Além disso, a Instrução CVM 558, estabelece que a Gestora encarregada de administrar carteiras de valores mobiliários deve cumprir com as seguintes regras de conduta: (i) desempenhar suas

atribuições de modo a atender aos objetivos de investimento do Investidor e evitar práticas que possam ferir a relação fiduciária mantida; (ii) exercer suas atividades com boa fé, transparência, diligência e lealdade em relação aos Investidores; (iii) cumprir fielmente o regulamento do fundo ou contrato firmado com o Investidor, prévia e obrigatoriamente por escrito, que deve conter as principais características dos serviços, tais como política de investimento, descrição detalhada da remuneração, riscos inerentes às operações, conteúdo e periodicidade das informações a serem prestadas, informações sobre outras atividades desenvolvidas pela Gestora no mercado e potenciais conflitos de interesses; (iv) transferir à carteira qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de gestor de carteira, observada a exceção aplicável a fundos de investimento prevista na Instrução CVM 555; (v) informar à CVM sempre que se verifique, no exercício de suas atribuições, a ocorrência ou indícios de violação da legislação e regulamentação que incumbe à CVM fiscalizar, no prazo máximo de 10 (dez) dias úteis; e (vi) estabelecer política relacionada à compra e venda de valores mobiliários por parte de Colaboradores e pela própria Gestora (vide Código de Ética).

A Gestora deve garantir, através de mecanismos de controle interno adequados, o permanente atendimento às normas e regulamentações vigentes, referentes às diversas alternativas e modalidades de investimento, à própria atividade de gestão de carteira e aos padrões de conduta ética e profissional.

2.2 Lei Anticorrupção Brasileira (Lei 12.846/13) e Decreto Regulamentar (8.420/2015)

A Lei Anticorrupção Brasileira vigente desde 01 de agosto de 2013 e respectivo Decreto Regulamentar 8.420, de 18 de março de 2015 (coletivamente "**Normas Brasileiras Anticorrupção**"), dispõem sobre a responsabilidade civil e administrativa de sociedades brasileiras ou estrangeiras que atuem no Brasil por conta de atos de seus diretores, gerentes, funcionários e outros agentes que atuem em nome da sociedade que envolvam a prática de corrupção contra a administração pública, nacional ou estrangeira, inclusive organizações públicas internacionais, como suborno e fraude em licitações e contratos administrativos da administração pública. Representantes de fundos de pensão públicos também devem ser considerados agentes públicos para os propósitos das Normas Brasileiras Anticorrupção.

Tais Normas Brasileiras Anticorrupção complementam a legislação penal aplicável para pessoas físicas.

Nos termos das Normas Brasileiras Anticorrupção, suborno significa prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada, incluindo os chamados “pagamentos facilitadores”.

Para que uma entidade seja condenada nos termos da Lei Anticorrupção, não é necessário comprovar a intenção ou má-fé do agente, apenas que o pagamento de suborno foi realizado ou oferecido.

Os Colaboradores e os Representantes devem questionar a legitimidade de quaisquer pagamentos requeridos por autoridade ou funcionário público que não contenha claro fundamento legal ou regulamentar.

Nenhum Colaborador ou Representante poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

Nos termos das Normas Brasileiras Anticorrupção, dentre outros cabíveis, a Gestora e os Representantes adotam os seguintes procedimentos internos e padrões de conduta a fim de minimizar os riscos de ocorrência de práticas de corrupção envolvendo seus Colaboradores e Representantes:

I - comprometimento da alta direção, incluídos os conselhos e comitês, em especial o Comitê de Risco e *Compliance*, evidenciado pelo apoio visível e inequívoco às Normas Brasileiras Anticorrupção;

II - padrões de conduta, políticas e procedimentos de integridade aplicáveis a todos os Colaboradores e Representantes, independentemente de cargo ou função exercidos;

III - treinamentos periódicos sobre o programa de integridade e sobre as Normas Brasileiras Anticorrupção;

IV - análise periódica de riscos para realizar adaptações necessárias ao programa de integridade;

V - registros contábeis que reflitam de forma completa e precisa as transações;

VI - controles internos que assegurem a pronta elaboração e confiabilidade de relatórios e demonstrações financeiras;

VII - procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, tal como pagamento de tributos, sujeição a fiscalizações, ou obtenção de autorizações, licenças, permissões e certidões;

VIII - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e fiscalização de seu cumprimento, em especial do(a) Diretor(a) de Risco e *Compliance* e do Comitê de Risco e *Compliance*;

IX - medidas disciplinares em caso de violação do programa de integridade;

X - procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;

XI - diligências apropriadas para contratação e, conforme o caso, supervisão, de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;

XII - a M Square envidará seus melhores esforços para incluir a previsão de cláusula anticorrupção expressa em todos os contratos que tenham por objeto a contratação de terceiro que preste serviços diversos à Gestora;

XIII - sempre que possível e aplicável, a M Square deverá estender a aplicação desta Política ao terceiro contratado, ou assegurar que ele cumpra diretrizes internas similares;

XIV - manutenção de alto padrão de governança nas relações comerciais mantidas com terceiros contratados ou quaisquer outros com quem a Gestora venha a ter relacionamento;

XV - verificação, durante processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades;

XVI - monitoramento contínuo do programa de *Compliance* e das normas aqui previstas, visando assegurar que continuam efetivas na prevenção, detecção e combate à ocorrência dos atos lesivos contra a administração pública; e

XVII - transparência quanto a doações para candidatos e partidos políticos.

Os procedimentos e padrões de conduta acima descritos serão usados pelas autoridades brasileiras para fins de dosimetria das sanções aplicáveis, caso a Gestora esteja envolvida, de alguma forma, em casos de corrupção decorrente de conduta de seus Colaboradores e Representantes.

Os Colaboradores e Representantes devem comunicar imediatamente a(o) Diretor(a) de Risco e *Compliance* em caso de violação ou suspeita de violação das Normas Brasileiras Anticorrupção, através do e-mail *Compliance*@msquare.com.br. Se o(a) Diretor(a) de Risco e *Compliance* estiver envolvido(a) em tal prática ou suspeita, as medidas disciplinares serão determinadas pelos sócios da M Square.

2.3 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* tem um dever contínuo, perante todos os Colaboradores, de proteger os interesses de cada Veículo de Investimento e Investidor. O(A) Diretor(a) de Risco e *Compliance* determinará, com relação às revisões das atividades operacionais da Gestora, se a Gestora está satisfazendo suas obrigações fiduciárias e não priorizando seus interesses próprios em detrimento daqueles dos Veículos de Investimento.

Para tal finalidade, o(a) Diretor(a) de Risco e *Compliance* avaliará determinadas atividades, tais como:

- Investimentos pessoais dos Colaboradores (vide Código de Ética);
- Atividades externas desenvolvidas por cada Colaborador (vide Código de Ética);
- Declarações feitas pela Gestora ou seus Colaboradores nos materiais de marketing e propaganda; e
- A estrutura de Taxas cobradas dos Veículos de Investimento (em especial as taxas de performance), de forma a mitigar a existência de conflitos de interesses.

3. Conflitos de Interesses

3.1 Introdução

É política da Gestora que todos os Colaboradores atuem de boa-fé e nos melhores interesses da Gestora, dos Veículos de Investimento e dos Investidores. Para essa finalidade, os Colaboradores não devem se colocar ou colocar a Gestora em uma posição que crie a aparência de impropriedade. Nenhum Colaborador poderá representar a Gestora em qualquer circunstância em que um interesse possa comprometer ou afetar sua capacidade de representar os interesses da Gestora de forma justa e imparcial.

Um "**conflito de interesse**" é uma situação em que alguém em uma posição de confiança tem um interesse profissional ou pessoal concorrente. Um conflito de interesse pode prejudicar a capacidade de um indivíduo de conduzir seus deveres e responsabilidades objetivamente. Nos casos em que os interesses dos Veículos de Investimento estiverem envolvidos, os Veículos de Investimento devem ter prioridade sobre os interesses dos Colaboradores. É política da Gestora buscar evitar conflitos de interesse, sempre que possível ou, caso seja inevitável, realizar ampla divulgação aos seus Investidores e obter o consentimento dos mesmos, conforme apropriado.

3.2 Identificando Conflitos de Interesses

Para que a Gestora trate um conflito de interesse, o conflito deve primeiramente ser identificado. Para tal finalidade, os Colaboradores são exigidos a relatar qualquer conflito de interesse potencial ou efetivo a(o) Diretor(a) de Risco e *Compliance*.

Segue uma descrição de exemplos de conflitos de interesse que podem surgir no contexto das atividades da Gestora:

3.2.1 Conflitos entre a Gestora e seus Veículos de Investimento

Um conflito de interesse pode existir se a Gestora tiver interesses conflitantes com os de seus Veículos de Investimento, como por exemplo, potencialmente, na alocação de custos e despesas entre si e seus Veículos de Investimento.

3.2.2 Conflitos entre Colaboradores e os Veículos de Investimento

Um conflito de interesse também pode existir se um Colaborador tiver um interesse concorrente com os Veículos de Investimento. Tal conflito poderá surgir, por exemplo, com relação aos investimentos pessoais de um Colaborador que concorra com ou possa afetar a atividade de investimento dos Veículos de Investimento. Além disso, os conflitos poderão surgir com relação a presentes dados a um Colaborador, bem como contribuições políticas feitas por um Colaborador.

3.2.3 Conflitos entre os Veículos de Investimento

Um conflito de interesse poderia existir caso a Gestora tenha múltiplos Veículos de Investimento com interesses concorrentes. Por exemplo, a Gestora pode enfrentar um conflito ao alocar as oportunidades limitadas de investimento entre seus múltiplos Veículos de Investimento.

3.2.4 Conflitos entre Investidores

Um conflito de interesse pode surgir entre Investidores nos Veículos de Investimento. Por exemplo, determinados Investidores no mesmo Veículo de Investimento poderão receber tratamento diferenciado de outros Investidores, incluindo liquidez preferencial ou direitos de informação.

3.2.5 Conflitos com Atividades e Negócios Externos

Um conflito de interesse pode surgir quando um Colaborador se envolver em atividades e negócios externos (vide Código de Ética), dependendo de sua posição na Gestora e a relação da Gestora com a atividade em questão. Atividades externas também podem acarretar potenciais conflitos de interesse nos casos em que o Colaborador se vir obrigado a escolher entre tal interesse e os interesses da Gestora ou dos Veículos de Investimento.

3.3 Procedimentos Operacionais e Revisão de *Compliance*

A Gestora identificou determinados conflitos de interesse potenciais e efetivos e implantou políticas e procedimentos para garantir que todos os Investidores e Veículos de Investimento sejam tratados de forma justa. Tais políticas e procedimentos estão contidos neste Manual; as políticas e procedimentos que disciplinam as atividades de investimento pessoal dos Colaboradores estão descritos no Código de Ética. Além disso, para cumprir sua obrigação fiduciária perante seus Veículos de Investimento, a Gestora divulga a seus Investidores todos os conflitos de interesse materiais potenciais e efetivos.

Todos os conflitos de interesse devem ser trazidos à atenção do(a) Diretor(a) de Risco e *Compliance*. Os conflitos e suas soluções subsequentes serão documentados pelo(a) Diretor(a) de Risco e *Compliance*. Além disso, diversos registros são mantidos pela Gestora para garantir a documentação adequada dos possíveis conflitos. Caso o conflito se refira a(o) o(a) Diretor(a) de Risco e *Compliance*, esta deverá levar a questão aos demais membros do Comitê de Risco e *Compliance* da M Square.

4. Ofertas e *Suitability* do Investidor

4.1 Regulamentações de *Suitability* no Brasil

Embora potencialmente autorizada pela Instrução CVM 558, a Gestora não tem a intenção de distribuir ou ofertar os Fundos CVM para o mercado e, portanto, não estará sujeita às regras de distribuição estabelecidas na Instrução CVM 539 de 13 de novembro de 2013, conforme alterada ("**Instrução CVM 539**"), e outras normas aplicáveis às atividades de distribuição.

Neste sentido, como os administradores fiduciários e distribuidores dos Fundos CVM manterão a relação comercial com os Investidores, consequentemente serão eles os principais responsáveis por determinar a adequação dos investimentos ao perfil do Investidor (*suitability*).

Nesse contexto, a Instrução CVM 539, que trata dos procedimentos de *suitability* que devem ser adotados com relação a clientes ou potenciais clientes de produtos, serviços ou operações financeiras no Brasil, determina expressamente que o administrador fiduciário e distribuidor, entre outras obrigações, deverá verificar se:

I – o produto, serviço ou operação é adequado aos objetivos de investimento do Investidor;

II – a situação financeira do Investidor é compatível com o produto, serviço ou operação; e

III – o Investidor possui conhecimento necessário para compreender os riscos relacionados ao produto, serviço ou operação.

Sem prejuízo do fato de a M Square não pretender distribuir ou ofertar os Fundos CVM para o mercado, permanecendo apenas como gestora das carteiras dos Fundos CVM, a Gestora cooperará com os administradores fiduciários e distribuidores para identificar os Investidores e manter seus registros atualizados em conformidade com o Anexo I da Instrução CVM 301 de 16 de abril de 1999, conforme alterada (“**Instrução CVM 301**”).

4.2 Procedimentos Operacionais e Revisão de *Compliance*

Nos casos em que tiver acesso direto ao cadastro dos Investidores, é política da Gestora somente aceitar Investidores que acredite serem adequados para tornarem-se Investidores (com base na situação financeira do investidor, experiência de investimento e objetivos de investimento).

Como parte de sua implantação do processo de *suitability* de Investidores da M Square, o qual é de responsabilidade dos distribuidores, quando, excepcionalmente, a Gestora receber o contato direto do cliente e sua ficha cadastral, a Gestora cooperará com os administradores fiduciários e distribuidores com a finalidade de: (i) coletar informações para avaliar o nível de conhecimento do Investidor com relação aos mercados de capitais e financeiros e os produtos disponíveis; (ii) notificar o Investidor com relação aos riscos em suas alocações existentes de investimento, de modo a aumentar a ciência de seus limites para os mesmos; (iii) explicar ao Investidor os procedimentos para monitorar os investimentos e apresentar relatórios com a frequência acordada; e (iv) quando aplicável, obter o consentimento do Investidor para adaptar o perfil de investimento para quaisquer novas circunstâncias que o afetem, caso o distribuidor não o faça.

5. Manutenção de livros e registros

5.1 Introdução

Todos os documentos, dados de operações, livros e registros exigidos devem ser mantidos em conformidade com a Lei Aplicável, incluindo regulamentações promulgadas pela CVM e ANBIMA.

Em conformidade com o artigo 16, IV, da Instrução CVM 558, a Gestora deve manter todos os documentos atualizados relacionados às operações com valores mobiliários que compõem os portfólios sob sua gestão, em perfeita ordem e disponíveis ao Investidor.

Além disso, a Instrução CVM 555 de 17 de dezembro de 2014, conforme alterada (“**Instrução CVM 555**”), estabelece que a administração dos Fundos CVM compreende o conjunto de serviços relacionados

direta ou indiretamente ao funcionamento e manutenção dos Fundos CVM que podem ser fornecidos pelo próprio administrador fiduciário ou por terceiros contratados por ele por escrito em nome de cada Fundo CVM. Neste sentido, o administrador fiduciário contrata a Gestora, como um terceiro autorizado, para a gestão do portfólio dos Fundos CVM.

O administrador fiduciário é o principal responsável pelo funcionamento e manutenção dos Fundos CVM, e de acordo com o artigo 90 da Instrução CVM 555, o administrador deve manter atualizados e em perfeita ordem: (i) o livro de registro de Investidores; (ii) o livro de atas de assembleia geral, incluindo a lista de presença; (iii) o parecer de auditor independente; (iv) o registro contábil referente às operações do fundo e seus ativos; e (v) os documentos referentes às operações do fundo, por um período de 5 (cinco) anos.

5.2 Registros Típicos de Atividades

Os registros típicos de atividade incluem, porém sem limitação, talões de cheque, extratos bancários e reconciliações; os contratos escritos celebrados pelo gestor de recursos de terceiros; todas as faturas ou extratos relacionados ao negócio do gestor de recursos de terceiros; e todos os recibos de dinheiro e diários de gasto, livro-razão adequado, todos os balancetes comerciais, demonstrações financeiras e papéis de auditoria interna.

5.3 Registros Adicionais

Os registros adicionais incluem, porém sem limitação: um registro de cada ordem dada pelo gestor para a compra ou venda de um valor mobiliário; todas as comunicações escritas recebidas e enviadas pela Gestora relacionadas a (i) qualquer recomendação ou parecer feito ou proposto, (ii) qualquer recibo, gasto ou entrega de recursos ou valores mobiliários, e (iii) a colocação ou execução de qualquer ordem para a compra ou venda de um valor mobiliário; cópias dos manuais e procedimentos escritos, inclusive este Manual e quaisquer aditamentos ao mesmo; registros de quaisquer violações do Código de Ética e de qualquer ação tomada; e todas as comunicações e materiais de marketing destinados ao Investidor.

5.4 Períodos de Arquivamento

Os livros e registros devem ser mantidos e preservados em um local facilmente acessível por um período não inferior a 5 (cinco) anos a partir do final do ano fiscal aplicável durante o qual o último lançamento foi feito em tal registro, sendo que os dois anos mais recentes devem ser mantidos no escritório da Gestora. Os documentos de constituição da Gestora e quaisquer aditamentos aos mesmos devem ser mantidos por pelo menos três anos após o término da Gestora.

5.5 Registros Eletrônicos

Os registros poderão ser mantidos em mídia de armazenamento eletrônico. Um gestor de recursos de terceiros armazenando os registros em mídia eletrônica deve estabelecer e manter procedimentos para: (i) preservar os registros e protegê-los de perda, alteração ou destruição; (ii) razoavelmente garantir que qualquer reprodução dos registros em papel para mídia eletrônica seja exata; e (iii) limitar o acesso ao pessoal autorizado.

5.6 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* conduzirá e documentará as revisões garantindo que todos os livros e registros necessários estejam sendo mantidos.

6. Propaganda e Marketing

6.1 Introdução

A regulamentação brasileira estabelece exigências e condições para propaganda e marketing com relação aos contatos feitos por qualquer Colaborador com terceiros. Esta Política de Propaganda e Marketing ("Política") formaliza os procedimentos inerentes à elaboração, divulgação e publicação de materiais de comunicação com investidores e marketing da Gestora e dos Veículos de Investimento.

Considerando que a M Square não fará a distribuição de cotas dos seus Veículos de Investimento, quando se tratar de captação de novos cotistas, os materiais referidos nesta Política deverão ser encaminhados para o(s) Distribuidor(es) responsável(is), ficando este(s) responsável(is) pelo envio e distribuição desses materiais aos potenciais Investidores. Nos casos de Investidores que já sejam cotistas da M Square, tais materiais poderão ser enviados diretamente pela Gestora, de forma a propiciar a manutenção do relacionamento com o Investidor, ou por meio do Distribuidor.

6.2 Propaganda e Marketing no Brasil

Embora a M Square não pretenda distribuir e ofertar os Fundos CVM para o mercado, no caso de a Gestora produzir materiais de marketing relacionados aos Fundos CVM, tais materiais deverão ser preparados em conformidade com as regras da CVM e o Código ANBIMA de Administração de Recursos de Terceiros (disponível em www.anbima.com.br) ("Código ANBIMA") e eventuais normativos aplicáveis, para o uso da própria M Square ou dos distribuidores dos Fundos CVM. Todos os materiais de marketing (incluindo Material Publicitário e Material Técnico) devem ser previamente revisados e validados pelo(a) Diretor(a) de Risco e *Compliance*. Sujeito às outras regras contidas no Código ANBIMA e Diretrizes da ANBIMA aplicáveis, o Capítulo V, Seção V da Instrução CVM 555

estabelece que o material de divulgação de um Fundo CVM, bem como as informações a ele relevantes, não podem estar em desacordo com o regulamento, lâmina de informações essenciais (caso aplicável) ou quaisquer outros documentos registrados na CVM. Qualquer material de divulgação de Fundo CVM deve ser identificado como sendo um material de divulgação e deverá mencionar a existência do regulamento e da lâmina de informações essenciais (se aplicável), bem como o website no qual tais documentos podem ser obtidos pelo Investidor. Nenhum material de divulgação pode assegurar ou sugerir a existência de garantia de resultados futuros ou isenção de risco para o Investidor. Qualquer divulgação de informação sobre os resultados do fundo só pode ser feita, por qualquer meio, após um período de carência de 6 (seis) meses da data da primeira emissão de cotas. Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade do fundo, deve obrigatoriamente: (i) mencionar a data de inicio de seu funcionamento; (ii) contemplar, adicionalmente à informação divulgada, a rentabilidade mensal e acumulada nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; (iii) ser acompanhada do valor do patrimônio líquido médio mensal dos últimos 12 (doze) meses ou desde sua constituição, se mais recente; (iv) divulgar o valor da taxa de administração e da taxa de performance, se houver, expressa no regulamento vigente nos últimos 12 (doze) meses ou desde sua constituição, se mais recente; e (v) destacar o publico alvo do fundo e as restrições quanto à captação. Sempre que o material de divulgação apresentar informações referentes à rentabilidade ocorrida em períodos anteriores, deve ser incluída uma advertência, com destaque, de que: (i) a rentabilidade obtida no passado não representa uma garantia de resultados futuros; e (ii) os investimentos nos fundos não são garantidos pelo administrador fiduciário, ou por qualquer mecanismo de seguro ou, ainda, pelo fundo garantidor de crédito (FGC).

Na Reunião de Treinamento de *Compliance* Anual, o(a) Diretor(a) de Risco e *Compliance*revisará as leis federais, regras e regulamentações aplicáveis a valores mobiliários no que diz respeito aos materiais de marketing dos Fundos CVM. O(A) Diretor(a) de Risco e *Compliance* também poderá conduzir uma reunião periódica de *Compliance* quando qualquer nova lei, regra ou regulamentação entrar em vigor para explicar e educar os Colaboradores com relação a quaisquer alterações.

O(A) Diretor(a) de Risco e *Compliance* revisará todos os materiais de marketing para determinar a conformidade com as Leis Aplicáveis. Especificamente, o(a) Diretor(a) de Risco e *Compliance* sempre buscará garantir que quaisquer materiais promocionais não façam promessas indevidas ou passem uma mensagem errada ao receptor e contenham todas as ressalvas adequadas. O(A) Diretor(a) de

Risco e *Compliance* aprovará todos os materiais de marketing e manterá os mesmos em um arquivo de material de marketing aprovado propriamente designado.

6.3 Política de Materiais de Propaganda e Marketing

Todos os materiais de marketing devem ser justos e corretos e incluir as ressalvas adequadas referentes aos riscos de investimento nos Veículos de Investimento e outras ressalvas que possam ser adequadas.

Esta Política tem por objetivo formalizar os procedimentos inerentes à elaboração e divulgação de materiais de comunicação com Investidores e marketing da Gestora e dos Veículos de Investimento, sejam esses documentos entregues em vias físicas em visitas pessoais, encaminhados através de e-mails, malas diretas, objeto de apresentações em *roadshows* e eventos ou outros.

6.3.1 Diretrizes Gerais

Para fins da legislação em vigor e desta Política, considera-se publicidade toda comunicação que tenha por objeto propaganda institucional e estratégia mercadológica dos Veículos de Investimento, entre a Gestora e Investidores ou potenciais Investidores, por meio de mídia pública disponibilizado em locais públicos, mala direta, e-mail *marketing*, ou quaisquer outros veículos e sítios públicos (televisivo, impresso, radiofônico, digital, audiovisual e tecnologias que possam surgir), observadas as definições abaixo.

De acordo com o Código ANBIMA, Publicidade pode ser dividida entre:

(i) Material Publicitário: material sobre os Fundos CVM ou sobre a atividade de gestão de recursos divulgado pela Gestora por qualquer meio de comunicação disponível, que seja destinado a investidores ou potenciais investidores, com objetivo de estratégia comercial e mercadológica (por exemplo, podem inclusive ser divulgações mais curtas e simples, chamadas para o produto, por qualquer mídia, inclusive meio digital, vídeos, banners, SMS, plataformas, mídias sociais, etc.); e

(ii) Material Técnico: material sobre Fundos CVM divulgado pela Gestora por qualquer meio de comunicação disponível, que seja destinado a investidores ou potenciais investidores com o objetivo de dar suporte técnico a uma decisão de investimento, devendo conter, no mínimo, as seguintes informações: (a) descrição do objetivo e/ou estratégia; (b) público-alvo, quando destinado a investidores específicos; (c) carência para resgate e prazo de operação; (c) tributação aplicável; e (d) informações sobre os canais de atendimento. Essas informações serão também mantidas nas

dependências da Gestora, à disposição dos interessados, seja por meio impresso ou passível de impressão.

Ao divulgar Material Publicitário, em qualquer meio de comunicação disponível, a Gestora deve incluir, em destaque, link ou caminho direcionando os investidores ou potenciais investidores ao Material Técnico sobre o Fundo CVM mencionado, de modo que haja conhecimento de todas as informações, características e riscos do investimento. Nesse caso, não precisaria, assim, incluir avisos obrigatórios, uma vez que o material técnico conteria as informações técnicas e os requisitos necessários.

No entanto, se já constar do Material Publicitário todos os requisitos do Material Técnico, tal caminho deixa de ser obrigatório. Ressalta-se, ainda, que se a Gestora fizer menção de seus Fundos CVM nos Materiais Publicitários de forma geral e não específica, deve também incluir link ou caminho que direcione os Investidores (atuais ou potenciais) para o seu website.

Toda comunicação com Investidores e *marketing* da Gestora ou dos Veículos de Investimento que se enquadre no conceito de Material Publicitário ou Material Técnico deve obedecer às diretrizes mencionas nesta Política.

6.3.2 São exemplos de Material Publicitário e Material Técnico

- Qualquer material, encaminhado através de mala-direta, com caráter não exclusivo, como por exemplo, relatórios de informações mensais sobre os Fundos CVM;
- Qualquer material, encaminhado em caráter exclusivo, diretamente ao e-mail do Investidor que não expressamente mencionado no item 6.3.3 abaixo;
- As pautas e apresentações institucionais ou sobre produtos, usadas para contato direto, com objetivo comercial e fruto de estratégia de negócio;
- Boletins e comunicados em geral;
- Apresentações, descrições de produtos, comentários sobre o mercado e todo o tipo de material escrito usado na promoção e ou no suporte à distribuição de produtos a Investidores ou potenciais Investidores;
- Todo e qualquer tipo de campanha publicitária veiculada em mídia nacional ou estrangeira, inclusive mídias sociais; e
- *Website* da Gestora.

6.3.3 Não são considerados Material Publicitário ou Material Técnico:

- Formulários cadastrais, questionários de perfil do Investidor ou perfil de investimento, materiais destinados à comunicação de alterações de endereços, telefones ou outras informações de simples referência para o Investidor;
- Materiais que se restrinjam a informações obrigatórias exigidas pela regulação vigente;
- Questionários de *due diligence* e propostas comerciais;
- Materiais de cunho estritamente jornalístico, inclusive entrevistas, divulgadas em quaisquer meios de comunicação;
- Divulgação continuada de cota, patrimônio líquido e rentabilidade por qualquer meio, bem como a divulgação da carteira na forma da política de divulgação prevista nos documentos dos Fundos CVM, incluindo respectivo Regulamento, Formulário de Informações Complementares e Lâmina de Informações essenciais, se houver;
- Saldos, extratos e demais materiais destinados à apresentação de posição de financeira, movimentação e rentabilidade, desde que restrito a estas informações ou assemelhadas;
- Propaganda de empresas do grupo econômico da Gestora que apenas faça menção aos Fundos CVM como um de seus produtos, o de departamentos e/ou empresas que realizam a administração fiduciária e gestão de recursos em conjunto com os outros departamentos ou empresa que desenvolvam outros negócios do grupo econômico;
- Materiais e/ou relatórios que tenham como finalidade mero acompanhamento do Fundo CVM (desde que seja um Fundo Exclusivo ou Reservado); e
- Demais materiais e informações na forma solicitada especificamente pelo Investidor.

As regras desta Política destinam-se, exclusivamente, às relações da Gestora com seus Investidores (atuais ou potenciais), não sendo aplicáveis entre a Gestora e seus Colaboradores no exercício de suas funções.

6.3.4 Processo de aprovação de Materiais Publicitários ou Materiais Técnicos

Todos os materiais de marketing e de comunicação com Investidores elaborados pela área responsável, deverão passar pelo seguinte procedimento:

✓ Deverão ser encaminhados, pelo e-mail *Compliance*@msquare.com.br, à área de *Compliance* para revisão. Em se tratando de materiais para Investidores e *prospects* brasileiros, o documento deverá ser encaminhado com antecedência razoável para que a área possa averiguar todo o conteúdo, realizar comentários, enviar para consultor externo, se necessário, verificar alterações e aprovar a minuta final;

✓ Em se tratando de materiais destinados a outras jurisdições, no início do projeto, a área de *Compliance* deverá ser envolvida para realizar levantamento de exigências legais e regulatórias aplicáveis na jurisdição almejada. O processo de análise de jurisdições estrangeiras poderá exigir consulta a especialistas estrangeiros;

✓ Após receber aprovação da área de *Compliance*, a área responsável deverá manter todo o histórico de informações e todas as versões e alterações do documento;

✓ Materiais-padrão, tais como relatórios mensais e periódicos e demais documentos já previamente aprovados, uma vez analisados pela área de *Compliance*, não precisam ser aprovados a cada utilização (isto é, desde que não haja conteúdo novo, mas apenas alteração nos números de taxas, PL, AUM, etc).

✓ A revisão dos materiais-padrão ocorrerá anualmente pela área de *Compliance* ou sempre que houver mudanças de conteúdo.

6.3.5 Solicitação de aprovação de Material ou Material Técnico

As solicitações de aprovações de materiais deverão ser encaminhadas à área de *Compliance*, através do e-mail *Compliance*@msquare.com.br e deverão ser aprovadas por escrito pela área de *Compliance*.

6.3.5.1 Responsabilidades

A área que elaborou o material é responsável: (i) por todo seu conteúdo técnico, (ii) pela identidade visual, (iii) pelo tipo de mídia a ser utilizada, (iv) por destacar o público alvo, objeto da apresentação; (v) por incluir fonte e data em todas as imagens, gráficos, tabelas e referências utilizadas; e (vi) por submeter o material para revisão da área de *Compliance*. É necessário que fontes das informações públicas ou de terceiros sejam incluídas no material sempre que aplicável.

A área responsável pela elaboração do material (e os Colaboradores envolvidos) responderá por ele junto aos órgãos reguladores e autorreguladores, bem como perante o mercado e a concorrência. Por isso, não devem jamais utilizar informações infundadas, não verídicas, copiadas de terceiros, ou dissonantes com o regulamento, lâminas e demais documentos dos Fundos CVM.

6.3.6 Diretrizes para confecção e distribuição de Material Publicitário ou Material Técnico

- Produzir materiais adequados aos investidores, minimizando incompreensões quanto ao seu conteúdo e privilegiando informações necessárias para a tomada de decisão;
- Não devem utilizar hipérboles e superlativos não comprovados e devem ter conteúdo claro, buscando sempre a interpretação feita pelo “homem médio”;

- Devem ser elaborados em linguagem simples, clara, objetiva e adequada, buscando transparência e precisão, de modo a não induzir a erro ou a decisões equivocadas de investimentos, advertindo seus leitores para os riscos do investimento;
- Todos os documentos devem ter seu público-alvo especificado;
- Não devem conter qualificações injustificadas ou em desacordo com esta Política, opiniões para as quais não exista base razoável ou previsão de eventos futuros sem base técnica; Que contenham gráficos: tenham título, descrição dos dados constantes nos eixos e sejam datados;
- Que contenham referências externas: sigam com fonte e data;
- Que contenham Notas de Rating sobre empresas, países e ativos: sigam com a respectiva data e nome da empresa de Rating;
- Devem conter informações verdadeiras, completas, consistentes e alinhadas com o Regulamento, a Lâmina de Informações Essenciais (caso aplicável) e demais documentos dos Fundos CVM, bem como observar integralmente o disposto no item 6.2. acima;
- Não devem assegurar, prometer ou sugerir a existência de promessas de rentabilidade, garantia de resultado e a isenção de risco;
- Devem acompanhar todos os alertas regulatórios e autorregulatórios, sobretudo aqueles advindos das Instruções da CVM e do Código ANBIMA;
- Disponibilizar informações que sejam pertinentes ao processo de decisão, sendo tratados de forma técnica assuntos relativos à performance passada, de modo a privilegiar as informações de longo prazo em detrimento daquelas de curto prazo;
- Manter a mesma linha de conteúdo e forma e, na medida do possível, incluir a informação mais recente disponível, de maneira que não sejam alterados os períodos de análise, buscando ressaltar períodos de boa rentabilidade, descartando períodos desfavoráveis, ou interrompendo sua recorrência e periodicidade especialmente em razão da performance;
- Toda informação divulgada por qualquer meio, na qual seja incluída referência à rentabilidade dos Fundos CVM, deve obrigatoriamente obedecer ao disposto sobre o tema na regulamentação da CVM e ANBIMA;
- Privilegiar dados de fácil comparabilidade, e, caso sejam realizadas projeções ou simulações, detalhar todos os critérios utilizados, incluindo valores e taxas de comissões;
- Zelar para que haja concorrência leal, de modo que as informações disponibilizadas ou omitidas não promovam determinados fundos ou gestoras em detrimento de seus concorrentes, sendo permitida comparação conforme previsto nesta Política; e

- Todas as versões finais de materiais produzidos deverão ser mantidos por um período não inferior a 5 (cinco) anos.

6.3.7 Diretrizes para confecção de Qualificações

De acordo com o Código ANBIMA, são consideradas qualificações: quaisquer premiações, rankings, títulos, análises, relatórios ou assemelhados que qualifiquem os Fundos CVM e/ou a Gestora no exercício das atividades de gestão de recursos.

Nessa linha, ao divulgar uma qualificação, deverá considerar, cumulativamente:

- a última qualificação obtida, contendo a referência de data e a fonte pública responsável;
- as qualificações fornecidas por fontes públicas independentes da Gestora;
- similaridade entre os Fundos CVM, tais como tamanho, liquidez, regras de cotização, carência, classificação ANBIMA, e a similaridade com outras gestoras, se a qualificação fizer referência a esta;
- os dados dos Fundos CVM que sejam oriundos integralmente da base de dados ANBIMA, devendo ser explicitada a classificação ANBIMA dos Fundos analisados, quando aplicável;
- qualificações de períodos mínimos de doze meses;
- se, dentre os Fundos analisados, algum deles não estiver aberto para captação; e
- as taxas cobradas que não estejam refletidas no valor da cota dos Fundos analisados.

À Gestora, na divulgação de qualificações, é vedado:

- dar entendimento mais amplo do que o explicitamente declarado na qualificação
- adicionar qualquer material analítico (quantitativo ou qualitativo) que não faça parte do original da qualificação;
- incluir qualificação que não esteja vinculada à Gestora e/ou aos Fundos CVM; e
- incluir qualificação injustificadas ou que faça uso de padrões de divulgação de rentabilidade que estejam em desacordo com o disposto nesta Política ou normativos aplicáveis.

6.3.8 Diretrizes para Comparação e Simulação, Histórico de Rentabilidade, Avisos Obrigatórios e Selos

Na elaboração de Material Técnico, é permitida a comparação entre fundos de investimento, entre as instituições e as atividades de administração fiduciária e gestão de recursos, contanto que sejam seguidas as regras dos normativos aplicáveis e do Código ANBIMA para tanto. Não pode haver comparação em Material Publicitário.

Dentre os requisitos previstos, estão a necessidade de se respeitar a concorrência legal e de que a comparação não contenha juízo de valor. Também devem estar presentes todos os elementos mínimos para Material Técnico, conforme constante da definição acima, e devem ser divulgados comparativos de rentabilidade para todos os fundos comparados nas hipóteses em que tenham parâmetros distintos em suas políticas de investimento e cobrança de taxa de performance.

Também deverão ser observadas as regras sobre divulgação de histórico de rentabilidade previstas no Código ANBIMA e demais diretrizes da ANBIMA, inclusive, dentre outros aspectos, quanto aos intervalos de tempo, à segregação dos Fundos 555 dos demais, o valor do patrimônio líquido conforme previsto e, no caso de divulgação de rentabilidade diária, ao cumprimento dos requisitos específicos.

Por fim, a Gestora deverá atentar para a inclusão com destaque dos avisos obrigatórios previstos no Código ANBIMA no Material Publicitário ou Material Técnico e no Formulário de Informações Complementares dos Fundos CVM, bem como observar o disposto na diretriz da ANBIMA sobre selos e em quaisquer outras que sejam aplicáveis.

7. Comunicações com o público

7.1 Políticas de Comunicações com o Público

É política da Gestora que todas as comunicações com o público, Investidores e Investidores potenciais, seja com base no princípio da boa-fé e forneça uma base idônea para avaliar os méritos de qualquer Veículo de Investimento gerido pela Gestora. Nenhum fato material ou qualificação poderá ser omitido. Se a omissão, à luz do contexto em que o material é apresentado, resultar com que os materiais de propaganda ou marketing sejam enganosos, as declarações ou reivindicações exageradas, não garantidas ou enganosas não serão usadas em qualquer forma de comunicação feita pela Gestora ou qualquer Colaborador. Além do mais, a Gestora não publicará, circulará ou distribuirá, direta ou indiretamente, qualquer comunicação ou material que a Gestora saiba ou tenha motivo para saber que contém quaisquer declarações falsas de fato material ou sejam de outro modo falsas ou enganosas.

7.1.1 Meios de Comunicação

Os representantes da M Square junto aos meios de comunicação são, exclusivamente, o(a) Diretor(a) de Risco e *Compliance* e o(a) Diretor(a) de Investimentos que poderão delegar esta função sempre que julgarem adequado. Os demais Colaboradores somente poderão dar informações a terceiros

em geral, repórteres, entrevistadores ou jornalistas mediantes expressa autorização do(a) Diretor(a) de Risco e *Compliance*.

7.1.2 Salas de Chat

Os Colaboradores são proibidos de usar salas de chat com relação as suas atividades na Gestora e são proibidos de usar o computador da Gestora e sistema de rede para comunicarem-se através de salas de chat para questões pessoais.

7.1.3 Mídia Social

O uso de mídia social por Colaboradores (p.ex., *Facebook*, *Twitter*) com relação à Gestora e seu negócio deve seguir as regras aqui estabelecidas. Os Colaboradores poderão divulgar o nome da Gestora e seu cargo em sites de networking profissional (p.ex., *LinkedIn*), porém, ao assim fazer, o Colaborador deve: abster-se de quaisquer divulgações que possam prejudicar a Gestora ou qualquer Veículo de Investimento; não representar inadequadamente seu cargo, posição ou natureza de seu trabalho; e não postar comentários que poderão ser entendidos como um "depoimento" das atividades da Gestora.

7.1.4 Participação em Conferências

As informações apresentadas em uma conferência por um Colaborador são consideradas uma Propaganda ou Publicidade e sujeitas às regulamentações da CVM, ANBIMA, bem como potencialmente da jurisdição onde ela é veiculada, e/ou onde o Investidor reside geograficamente (vide Seção 6 – **PROPAGANDA E MARKETING**). Portanto, antes de um Colaborador participar de uma conferência, o mesmo deve ter ambos os materiais e conteúdo da apresentação aprovados pelo(a) Diretor(a) de Risco e *Compliance*.

7.2 Procedimentos Operacionais e Revisão de *Compliance*

A Gestora reserva o direito de monitorar e revisar toda a atividade conduzida pelos Colaboradores por meio dos sistemas de tecnologia da informação da Gestora para garantir adesão às políticas e procedimentos da Gestora. Isso inclui o direito de monitorar a participação em websites de mídia social e revisar quaisquer arquivos eletrônicos e mensagens armazenados ou transmitidas por meio dos sistemas da Gestora.

O(A) Diretor(a) de Risco e *Compliance* aprovará o conteúdo de quaisquer materiais a serem apresentados em uma conferência ou entrevista à imprensa e manterá um registro de todas as conferências e seu conteúdo.

8. Operações e melhor execução

8.1 Introdução

A Gestora busca defender os melhores interesses de seus Veículos de Investimento ao (i) tomar decisões adequadas de investimento à luz dos objetivos, necessidades e circunstâncias de investimento do Veículo de Investimento; e (ii) conduzir operações de uma forma que seja consistente com as Leis Aplicáveis.

Conforme descrito na Seção 3.1 acima, a Instrução CVM 558 estabelece que a Gestora deve cumprir com as regras de comportamento que incluem, entre outras: (i) desempenhar suas atribuições de modo a atender aos objetivos de investimento do Investidor e evitar práticas que possam ferir a relação fiduciária mantida; (ii) exercer suas atividades com boa fé, transparência, diligência e lealdade em relação aos Investidores; (iii) cumprir fielmente o regulamento do fundo ou contrato firmado com o Investidor, prévia e obrigatoriamente por escrito, que deve conter as principais características dos serviços, tais como política de investimento, descrição detalhada da remuneração, riscos inerentes às operações, conteúdo e periodicidade das informações a serem prestadas, informações sobre outras atividades desenvolvidas pela Gestora no mercado e potenciais conflitos de interesses; (iv) transferir à carteira qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de gestor de recursos, observada a exceção aplicável a fundos de investimento prevista na Instrução CVM 555. A M Square e seus Colaboradores devem evitar comportamentos que gerem a quebra da relação de confiança com Investidores de modo a prestar as informações que lhe forem solicitadas pelo Investidor pertinentes aos valores mobiliários integrantes da carteira gerida.

A Gestora deve garantir, através de mecanismos de controle interno adequados, o permanente atendimento às normas e regulamentações vigentes, referentes às diversas alternativas e modalidades de investimento, à própria atividade de gestão de recursos e aos padrões de conduta ética e profissional.

8.2 *Soft Dollars*

A Gestora atualmente não tem quaisquer acordos formais de *Soft Dollars*[1]. Caso venha a tê-los no futuro, o(a) Diretor(a) de Risco e *Compliance* deve garantir que todos os acordos estejam dentro do

[1] "*Soft Dollars*" significa um acordo em que produtos ou serviços, além da execução de *ordens*, são obtidos por um gestor de recursos de terceiros ou através de uma corretora em troca de direcionamento de ordens de operações de clientes à corretora.

escopo das normas e melhores práticas nacionais e internacionais, e devidamente documentadas, devendo tal prática ser informada no item próprio do Formulário de Referência da Gestora. Nesse caso, caberá a(o) Diretor(a) de Risco e *Compliance* assegurar a transparência aos investidores quanto a qualquer recebimento de serviços adicionais fornecidos pelas corretoras em razão de sua contratação e relacionamento. (Tratamento de Soft Dollar), incluindo as hipóteses em que tais benefícios poderão ser aceitos pela M Square, bem como hipóteses cujo recebimento seja vedado ou transponha os limites de sua utilização.

8.3 Melhor Execução

Em regra, um gestor de recursos de terceiros tem o dever de obter a "Melhor Execução" para as transações de seus Fundos CVM quando este estiver em uma posição de direcionar as ordens às contrapartes. A Melhor Execução é determinada no contexto de uma transação específica ou com relação às obrigações gerais de execução do gestor de recursos referentes aos ativos da carteira. Os elementos que definem Melhor Execução incluem: melhor preço (o melhor preço é considerado como o preço mais alto que uma carteira pode vender um valor mobiliário e o menor preço que uma carteira pode comprar um valor mobiliário); *timing* da execução; a qualidade da pesquisa fornecida; a receptividade da contraparte à Gestora; e os recursos financeiros da corretora.

Atualmente, a obrigação de Melhor Execução em relação ao uso de corretoras e buscar pelo melhor preço não é aplicável à M Square, tendo em vista a atual política de investimento da Gestora, de investir essencialmente em cotas de fundos de investimentos geridos e administrados por terceiros, sobretudo no exterior.

8.3.1 Lista de Contrapartes Aprovadas

Caso a M Square venha a utilizar corretoras para os investimentos em nome dos Fundos CVM, o(a) Diretor(a) de Risco e *Compliance* deverá manter uma "**Lista de Contrapartes Aprovadas**" com base nos critérios estabelecidos pela Gestora. Os *gestores* colocarão as ordens exclusivamente com corretoras constantes da Lista de Corretoras Aprovadas, exceto se o *gestor* receber a autorização prévia por escrito do(a) o(a) Diretor(a) de Risco e *Compliance* para usar outra contraparte. O(A)

Os gestores de recursos de terceiros que recebem tais produtos ou serviços tipicamente pagam as comissões de corretoras acima daquelas que seriam cobradas unicamente para a execução. O uso de *Soft Dollars* para comprar produtos e serviços pode criar um conflito de interesse.

Diretor(a) de Risco e *Compliance* atualizará a Lista de Contrapartes Aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

8.3.2 Revisão de Contrapartes

Quando aplicável, a equipe de gestão e o(a) Diretor(a) de Risco e *Compliance* devem rever o desempenho de cada contraparte e considerar, entre outros aspectos: a qualidade das execuções fornecidas; o custo das execuções; e potenciais conflitos de interesse.

8.3.3 Procedimentos Operacionais e Revisão de Compliance para Melhor Execução

Como parte de seus procedimentos para buscar a Melhor Execução, a Gestora somente aprovará contrapartes que ela determine que sejam capazes de fornecer a Melhor Execução para suas transações de Fundos CVM. As contrapartes que atendem essa norma são colocadas na Lista de Contrapartes Aprovadas. Os gestores farão um julgamento no momento da colocação de uma ordem sobre qual a melhor contraparte para fornecer a Melhor Execução considerando as características da transação.

8.4 Registro de Ordens de Operação

É política da Gestora que as transações sejam conduzidas da forma mais eficiente consistente com as diretrizes dos Veículos de Investimento e Leis Aplicáveis. A Gestora é obrigada a reter todos os registros relacionados à colocação e execução de transações para os Veículos de Investimento, independentemente do ativo alocado.

8.5 Erros Operacionais

A Gestora define um "**Erro Operacional**" como:

- Um erro no processo de tomada de decisão do investimento (p.ex., uma violação das diretrizes de investimento de um portfólio, compras feitas com caixa indisponível ou vendas feitas com valores mobiliários indisponíveis); e
- Um erro administrativo feito antes ou durante a execução da operação (p.ex., um Colaborador executa uma ordem para o valor mobiliário errado, ou para uma quantia incorreta ou número de ações).

8.5.1 Política de Erros Operacionais

É política da Gestora que os Erros Operacionais sejam corrigidos assim que possível após a descoberta em conformidade com os princípios e procedimentos abaixo descritos. O Comitê de Risco e *Compliance* determinará um método adequado para corrigir um Erro Operacional à luz de

todos os fatos e circunstâncias. Os Erros Operacionais não poderão ser resolvidos ao realocar o negócio para outro Veículo de Investimento. Os ganhos dos Erros Operacionais não poderão compensar perdas dos Erros Operacionais, exceto se as transações subjacentes constituam uma única transação. Os créditos por comissão, se houver, não poderão ser usados para pagar a correção dos Erros Operacionais.

8.5.2 Procedimentos Operacionais e Revisão de Compliance para Erros Operacionais

Os seguintes procedimentos devem ser seguidos para tratar os Erros Operacionais adequadamente:

- Quando um Erro Operacional for identificado, o Colaborador que identificar o erro deve prontamente relatá-lo o(a) Diretor(a) de Risco e *Compliance*.
- Todos os Erros Operacionais materiais devem ser documentados. O(A) Diretor(a) de Risco e *Compliance* determinará se um Erro Operacional é material e, se sim, determinará a resolução caso a caso. O(a) Diretor(a) de Risco e *Compliance* manterá cópias da documentação completa de Erro Operacional para fins de monitoramento e para fins regulatórios.
- Na medida em que um erro seja causado por um terceiro (tal como, um corretor ou administrador fiduciário), a M Square envidará seus melhores esforços para recuperar quaisquer perdas associadas a tal erro de tal terceiro.
- O(A) Diretor(a) de Risco e *Compliance* revisará os procedimentos de negociação para determinar se os procedimentos adicionais ou supervisão são necessários para evitar ou monitorar os Erros Operacionais.

9. Reclamações

9.1 Introdução

O(A) Diretor(a) de Risco e *Compliance* será responsável por garantir que todas as reclamações de Investidor ou de qualquer terceiro sejam tratadas em conformidade com as disposições desta Seção, bem como todas as Leis Aplicáveis.

9.2 Definição

Uma "**Reclamação**" é definida como qualquer declaração escrita ou oral de um Investidor ou qualquer pessoa atuando em nome de um Investidor alegando uma queixa com relação à solicitação ou execução de qualquer operação de valores mobiliários ou fundos de tal Investidor. As indagações de rotina ou expressões de preocupação sobre as condições de mercado ou cumprimento não são consideradas Reclamações.

9.3 Lidando com Reclamações

9.3.1 Responsabilidade de Colaboradores

Os Colaboradores devem notificar o(a) Diretor(a) de Risco e *Compliance* imediatamente ao ficarem cientes da existência de uma Reclamação, e fornecer a(o) Diretor(a) de Risco e *Compliance* todas as informações e documentações em sua posse relacionadas a tal Reclamação. Espera-se que os Colaboradores cooperem integralmente com a Gestora e todas as autoridades regulatórias na investigação de qualquer Reclamação.

9.3.2 Revisão pelo(a) Diretor(a) de Risco e Compliance

O(A) Diretor(a) de Risco e *Compliance* prontamente iniciará uma revisão das circunstâncias factuais acerca de qualquer Reclamação recebida e recomendará a ação adequada, se houver, aos sócios da M Square.

9.3.3 Procedimentos Operacionais e Revisão de Compliance

O(A) Diretor(a) de Risco e *Compliance* manterá um arquivo separado para todas as Reclamações em seu escritório principal. Os arquivos devem incluir as seguintes informações:

- Identificação da Reclamação;
- A data em que a Reclamação foi recebida;
- Identificação de cada Colaborador prestando serviço ao Veículo de Investimento ou Investidor;
- Uma descrição geral da Reclamação;
- Cópias de toda a correspondência envolvendo a Reclamação; e
- O resumo escrito da ação tomada com relação à Reclamação e sua resolução.

10. Política de confidencialidade e segurança da informação

10.1 Introdução

A "**Política de Confidencialidade e Segurança das Informações**" da Gestora estabelece o modo em que a Gestora cobra, utiliza e mantém as informações pessoais não públicas sobre seus Investidores[2] e o adequado gerenciamento das informações de posse temporária ou de propriedade da M Square. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

[2] A Política de Confidencialidade é projetada para cumprir com as obrigações da Gestora conforme a Instrução CVM 558 e demais orientações da CVM e Lei Complementar 105 de 2001, bem como a autorregulação da ANBIMA.

A responsabilidade em relação à confidencialidade e segurança da informação deve ser comunicada na fase de contratação dos Colaboradores e/ou início do vínculo com a Gestora, devendo os mesmos assinar o Compromisso de Responsabilidade e Confidencialidade na forma do Capítulo 9 do Código de Ética da Gestora, de forma manual ou eletrônica, excetuadas as hipóteses permitidas em lei. Os terceiros com os quais a Gestora compartilha Informações Pessoais Não Públicas de um Investidor (conforme definido abaixo) devem concordar por escrito em seguir as normas adequadas de segurança e confidencialidade, podendo tal documento ser excepcionado quando o contrato de prestação de serviço possuir cláusula de confidencialidade. A presente política aplica-se aos Investidores atuais e antigos Investidores.

É também obrigação de cada Colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação da área de *Compliance* em caso de qualquer dúvida.

10.2 Aviso de Política de Confidencialidade

De modo geral, a Gestora deve fornecer avisos claros e visíveis que refletem sua Política de Confidencialidade inicialmente a um Investidor no momento de estabelecer uma relação. A Lei Complementar 105 de 2001 e regras da CVM e ANBIMA são aplicáveis tanto para Investidores pessoas físicas quanto institucionais.

10.3 Divulgação das Informações Pessoais Não Públicas

"**Informações Pessoais Não Públicas**" significam as informações pessoalmente identificáveis que não estão publicamente disponíveis. As informações pessoalmente identificáveis incluem, entre outras coisas, o nome, endereço, número de cadastro de pessoa física de um indivíduo, informações de conta bancária e informações financeiras e de investimento. A Gestora coleta Informações Pessoais Não Públicas sobre seus Investidores por meio de documentos de subscrição, questionários de investidor e outras informações fornecidas pelo Investidor por escrito, pessoalmente, por telefone, eletronicamente ou por qualquer outro meio.

É política da Gestora exigir que todos os Colaboradores e aqueles prestando serviços em seu nome, mantenham as Informações Pessoais Não Públicas do Investidor como confidenciais. A Gestora não vende ou aluga Informações Pessoais Não Públicas dos Investidores e Veículos de Investimento. A Gestora não fornece as Informações Pessoais Não Públicas para terceiros afiliados ou não afiliados para fins de marketing.

A Gestora poderá compartilhar as Informações Pessoais Não Públicas nas seguintes situações:

- Para prestadores de serviço com relação à administração, prestação de serviço ou processamento de um Veículo de Investimento, caso o Investidor seja uma pessoa física e a Gestora seja o gestor de recursos de terceiros, que poderá incluir advogados, contadores, auditores e outros profissionais. A Gestora também poderá compartilhar informações com relação à prestação de serviço ou processamento das transações de Veículos de Investimento.
- Para responder uma intimação ou ordem judicial, processo judicial ou autoridades regulatórias;
- Para proteger conta fraude, transações não autorizadas (como, lavagem de dinheiro), e reivindicações de outros passivos; e
- Mediante o consentimento de um Investidor para liberar tais informações, incluindo a autorização para divulgar tais informações para pessoas atuando em uma qualidade fiduciária ou representativa em nome do Investidor.

10.4 Controles de Acesso

A M Square mantém proteções para defender as Informações Pessoais Não Públicas do Investidor e demais informações confidenciais, reservadas e privilegiadas da Gestora. A M Square restringe o acesso às informações pessoais e de conta do Investidor para aqueles Colaboradores que precisam saber tais informações no decorrer de suas responsabilidades de trabalho.

Nessa linha, todo acesso a diretórios e sistemas de informações da Gestora, inclusive ao acesso remoto e qualquer outro meio/veículo que contenha tais informações, deve ser controlado. Somente poderão ganhar tais acessos os Colaboradores previamente autorizados pela equipe de *Compliance*.

O controle do acesso a sistemas de informações da Gestora levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil;
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora; e
- Manutenção de documentos digitais de acordo com o disposto no item 10.5 abaixo e no Manual.

Os Colaboradores detentores de informações confidenciais, reservadas ou privilegiadas, em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

- Os Colaboradores devem evitar circular em ambientes externos à Gestora com cópias (físicas ou digitais) de arquivos contendo informações confidenciais, reservadas ou privilegiadas, salvo se

necessárias ao desenvolvimento do projeto e no interesse do cliente, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;

- Os materiais escritos contendo Informações Pessoais Não Públicas sobre os Veículos de Investimento e Investidores e demais informações confidenciais, reservadas e privilegiadas da Gestora devem ser fragmentados mediante descarte;
- O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico, e em meio físico trituradas em equipamentos adequados, nos termos do item 4.1.8 da Política de Segurança Cibernética da M Square;
- Os computadores, *laptops*, smartphones e outros dispositivos semelhantes contendo tais informações devem ter restrições de acesso em forma de senhas;
- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc;
- O disco rígido de quaisquer computadores e *laptops* antigos deve ser formatado antes de ser descartado, vendido ou doado;
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos; e
- A senha de acesso do Colaborador ao sistema da Gestora é pessoal e intransferível.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de *Compliance* sempre que necessário, devendo ser observado o disposto a esse respeito na Política de Segurança Cibernética da Gestora.

10.5 Proteção à Base de Dados

Os arquivos de Veículos de Investimento, dos Investidores e outras informações relacionadas a eles devem ser mantidos de uma forma segura, seja eletronicamente ou em armários traváveis de arquivamento. Os recursos computacionais da M Square devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções. .

Os arquivos de Veículos de Investimento, dos Investidores e outras informações relacionadas a eles devem ser mantidos de uma forma segura, seja eletronicamente ou em armários traváveis de arquivamento. Os recursos computacionais da M Square devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (*backups*) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela área de *Compliance*.

10.6 Identificação dos detentores da informação, manutenção de registros e logs

O(a) Diretor(a) de Risco e *Compliance* deve manter o registro dos Colaboradores que detenham informações privilegiadas, com a indicação do tipo de informação detida, devendo informar aos Diretores da Gestora todas as informações privilegiadas que estejam em poder dos Colaboradores que possam significar restrição nas operações da Gestora. Estas medidas foram desenvolvidas para evitar situações que possam suscitar um provável conflito de interesses ou a má utilização de informações. Desta forma, minimizando prováveis ameaças aos negócios e à imagem da Gestora.

Será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que os usuários (*login*) individuais de Colaboradores internos serão de responsabilidade do próprio e os usuários (*login*) de terceiros serão de responsabilidade da Diretora da área contratante. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

10.7 Vazamento de Informações Confidenciais

Os Colaboradores deverão comunicar à área de *Compliance* quaisquer casos de violações às normas de confidencialidade e segurança da informação que tenham conhecimento, mesmo que oriundos de ações involuntárias. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, o(a) Diretor(a) de Risco e *Compliance* discutirá com a equipe de TI qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos, levando o assunto à Diretoria, conforme o caso.

Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções: uso ilegal de *software*; introdução (intencional ou não) de vírus de informática; tentativas de

acesso não autorizado a dados e sistemas; ou compartilhamento ou divulgação de informações sensíveis da Gestora.

10.8 Treinamento, Testes de Segurança e Revisão de *Compliance*

A Gestora providenciará o treinamento dos Colaboradores com relação a essa política, mediante o início do vínculo com a Gestora. Além disso, na Reunião de Treinamento de *Compliance* Anual, o(a) Diretor(a) de Risco e *Compliance* explicará a Política de Confidencialidade e Segurança de Informação atual e atualizará e informará os Colaboradores de quaisquer alterações que surgirem com relação às Leis Aplicáveis ou quaisquer alterações que a Gestora possa fazer à Política de Confidencialidade e Segurança de Informação.

O treinamento visa assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui definidas, com a conscientização dos Colaboradores sobre segurança, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e falhas na interpretação das normas e procedimentos.

A Gestora realizará testes periódicos de segurança para os sistemas de informações (sem se limitar a, mas em especial, para os meios eletrônicos), no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação e para garantir que seus backups estejam funcionando e que a Gestora possa disponibilizar e-mails, caso solicitado por um regulador.

Esta política será revisada anualmente pela área de *Compliance* e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo, conforme análise e decisão do(a) Diretor(a) de Risco e *Compliance* / Comitê de Risco e *Compliance*. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

11. FATCA

11.1 Introdução

Em janeiro de 2013, a *Internal Revenue Service* ("IRS") publicou a regulamentação do *Foreign Account Tax Compliance Act* ("FATCA"), para auxiliar o governo dos Estados Unidos a coibir práticas de investimento no exterior que permitiam aos Investidores a evasão de impostos. O FATCA determina a retenção na fonte e reporte ao IRS por certas instituições financeiras americanas, bem como se estende para além dos Estados Unidos e estabelece que instituições financeiras estrangeiras ("FFIs")

como bancos, fundos offshore, certas corretoras, *trusts* e *trust companies* forneçam à IRS informações detalhadas sobre Investidores americanos.

FFIs deverão reportar-se anualmente à IRS ou à autoridade fiscal da jurisdição na qual residem, conforme o acordo firmado entre tal jurisdição estrangeira e os Estados Unidos. O método de reporte dependerá da jurisdição da FFI e de tal jurisdição ter firmado Acordo Intergovernamental ("IGA"). Adicionalmente, o tipo de IGA poderá também influenciar no processo de reporte.

11.2 Política de FATCA

É política da Gestora detectar, prevenir e reportar qualquer possível indício de evasão de impostos devidos aos Estados Unidos. A Gestora entende que a *due diligence* do Investidor e o reporte determinado pelo FATCA auxiliarão nesses esforços.

Adicionalmente, a Gestora tem por política não admitir Investidores residentes nos Estados Unidos mediante aporte em seus Veículos de Investimentos.

11.3 Procedimentos Operacionais e Revisão

A Gestora coordena esforços com os administradores fiduciários dos Veículos de Investimento para realizar as revisões de due diligence dos Investidores, conforme determinado pelo FATCA ou pelo IGA, visando confirmar sua residência fiscal. Adicionalmente, os procedimentos de aceitação de Investidores são constantemente revisados e supervisionado de forma a assegurar que (i) as informações pertinentes estão sendo obtidas em sua integralidade previamente à aceitação de qualquer investimento em fundo gerido pela Gestora e (ii) se tal potencial Investidor é um residente nos Estados Unidos para fins fiscais.

O(A) Diretor(a) de Risco e *Compliance* diligencia periodicamente, com o apoio dos membros do departamento técnico da Gestora dedicados às áreas de *Compliance* e Gestão de Riscos, para assegurar que os reportes dos administradores fiduciários dos Veículos de Investimento ao IRS estão sendo realizados tempestivamente e supervisiona as FFIs para verificar que estas cumprem os requisitos do FATCA (confirmando, assim, que os requerimentos do FATCA estão sendo pontualmente cumpridos pela FFI ou terceiro por esta contratado, tal como o administrador fiduciários do fundo / RTA).

Adicionalmente, o(a) Diretor(a) de Risco e *Compliance* certifica ao IRS, nos prazos exigidos, que a FFI mantém efetivos controles internos para cumprimento do FATCA, dependendo da jurisdição.

Importante ressaltar que a Gestora não possui Investidores residentes nos Estados Unidos e que não adota estruturas de fundo *master/feeder* para acomodar Investidores estrangeiros que desejem acessar investimentos no mercado brasileiro. Caso, a qualquer momento, a Gestora altere esta política e passe a admitir outros formatos para viabilização de investimentos por clientes residentes nos Estados Unidos na estratégia gerida pela Gestora, seus procedimentos serão revisitados pelo(a) Diretor(a) de Risco e *Compliance* para assegurar o pleno *Compliance* com as determinações do FATCA e IGA.

11.4 Designação de Diretora Responsável

A Gestora designou o(a) Diretor(a) de Risco e *Compliance* como o(a) Diretor(a) responsável para coordenar os esforços e assegurar o *Compliance* da Gestora com relação ao FATCA.

12. Plano de contingência e recuperação de desastre

12.1 Plano

A Gestora desenvolveu e implantou um plano de contingência e recuperação de desastre (“**Plano de Contingência**”), anexado a este Manual como o Anexo VII, a ser seguido pela Gestora no caso de um desastre (p.ex.: explosão, incêndio, inundação, terremoto, falha de energia) ou evento que prejudique o acesso aos sistemas da Gestora ou não permita acesso aos escritórios da Gestora na sua sede social.

12.2 Treinamento

Cada Colaborador receberá uma cópia do Plano de Contingência mediante seu ingresso na Gestora atualizado. Os Colaboradores serão treinados com relação ao Plano de Contingência pela equipe de TI da Gestora pelo menos anualmente.

12.3 Teste

A Gestora realizará um teste, uma vez ao ano, ou em prazo inferior se exigido pela Regulação em vigor, para garantir que o Plano de Contingência funciona efetiva e eficientemente e manterá registros escritos quanto ao desempenho do teste (funcionamento da tecnologia da informação necessária e dos sistemas de comunicação) e eventuais necessidades de revisão. O teste terá como objetivo também avaliar se o Plano de Contingência é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se podem ser ativados tempestivamente. Conforme as atividades da Gestora se desenvolvam e/ou se alterem, o(a)

Diretor(a) de Risco e *Compliance* diligenciará junto à equipe de TI da Gestora para que seja adaptado e atualizado o Plano de Contingência da Gestora, bem como acompanhará as evoluções da indústria de tecnologia para assegurar que a Gestora mantém um patamar adequado e atualizado de medidas, rotinas, softwares e infraestrutura nesta frente.

12.4 Procedimentos Operacionais e Revisão de *Compliance*

A Gestora conduzirá um teste do Plano de Contingência nos termos da Seção 12.3 acima. O(A) Diretor(a) de Risco e *Compliance* também revisará e atualizará o Plano de Contingência, conforme necessário, para garantir que esteja sempre devidamente atualizado.

ANEXO I

POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO

1.1. Objetivo

Lavagem de dinheiro é o ato de ocultar a verdadeira origem e titularidade dos frutos de atividade criminal internacionalmente reconhecida, tais como, crime organizado, tráfico de drogas ou terrorismo, de modo que os fundos aparentam vir de fontes legítimas. As pessoas que lavam dinheiro operam em todo o mundo e os fundos podem ser lavados através de muitos tipos diferentes de instituições financeiras, tais como, bancos, bancos de investimento e Gestoras de corretagem, e através de uma variedade de métodos, tais como, realização de múltiplos pequenos depósitos para evitar limites de relato (estruturação), movimentação de fundos através de entidades comerciais legítimas e estabelecimento de relações que ocultem a verdadeira relação ou fonte dos fundos.

Em conformidade com as regras estabelecidas pela Lei Federal Brasileira 9.613, datada de 3 de março de 1998, conforme alterada ("**Lei 9.613/98**"), e em conformidade com a Circular 3.461, datada de 24 de setembro de 2009, conforme alterada, e Carta Circular 3.542, datada de 12 de março de 2012, ambas elaboradas pelo Banco Central do Brasil, bem como a Instrução CVM 301 a Gestora e seus Colaboradores são proibidos de contratar ou prestar serviços de administração de carteira de valores mobiliários para quaisquer indivíduos, entidades, embarcações e países constantes na lista OFAC de Cidadãos Especialmente Designados, Pessoas Bloqueadas ou Lista de Países Sancionados ("**Lista SDN**") ou de outro modo identificados com relação a outros programas de sanções econômicas que o OFAC está encarregado de exercer. Diversos governos estrangeiros também proíbem a contratação ou fornecimento de benefícios financeiros ou serviços para indivíduos e entidades constantes na Lista SDN. Além disso, alertar uma pessoa que a polícia ou uma autoridade relevante está investigando ou planejando investigar um crime de lavagem de dinheiro ou atividades terroristas de financiamento é absolutamente proibido. Um Colaborador deve entrar em contato direta e tempestivamente com o(a) Diretor(a) de Risco e *Compliance* se suspeitar que um Investidor tenha praticado lavagem de dinheiro ou financiamento ao terrorismo ou caso verifique qualquer indício de lavagem de dinheiro nos investimentos efetuados pelos Veículos de Investimento.

1.2. Política Anti-Lavagem de Dinheiro

É política da Gestora buscar impedir, detectar e relatar qualquer incidente ou indício de possível lavagem de dinheiro. Para auxiliar nesse esforço, os Veículos de Investimento da Gestora possuem contratos com seus administradores fiduciários e distribuidores que obrigam tais prestadores de serviços a realizar verificações iniciais sobre os Investidores em potencial, antes deles investirem nos Veículos de Investimento geridos pela Gestora (incluindo, dentre outras medidas, por meio da devida identificação de clientes e manutenção de registros atualizados em conformidade com o Anexo I da Instrução CVM 301), sendo a plena satisfação destas verificações iniciais uma condição precedente e necessária para que o investimento seja aceito.

A M Square reconhece que é crime envolver-se em transações financeiras que envolvam lavagem de dinheiro, tanto sob a ótica da origem dos recursos investidos nos Veículos de Investimento sob sua gestão (passivo), quanto sob a ótica dos investimentos efetuados por tais Veículos de Investimento junto a contrapartes (ativo), sendo o “conhecimento efetivo” o padrão de conhecimento exigido. Dessa forma, será considerado que a Gestora detinha conhecimento da atividade ilícita caso ignore indícios que indicam ilegalidade ou não seja ativamente diligente em detectar tais indícios.

A Gestora deve comunicar o Conselho de Controle de Atividades Financeiras - COAF, dentro de um prazo máximo de 24 horas da ocorrência de quaisquer transações, ou propostas de transação, que possam constituir indicações de crimes referentes à "lavagem" ou ocultação de ativos, direitos e objetos de valor derivados de infrações penais, nos termos da Lei 9.613/98, incluindo terrorismo ou seu financiamento, ou relacionados a eles.

Adicionalmente, nos termos da Instrução CVM 534, a M Square deve fornecer à CVM uma declaração anual negativa atestando que não houve transações ou propostas de transações durante o ano anterior passíveis de comunicação, com base na Lei 9.613/98 e regulamentação aplicável, se este for o caso.

1.3. Rotinas de Fiscalização e Monitoramento de Contrapartes

1.3.1. Monitoramento de clientes dos Veículos de Investimento (Passivo)

Sob a ótica de monitoramento dos seus Investidores, a Gestora envidará seus melhores esforços para manter com os administradores fiduciários e distribuidores dos Veículos de

Investimento os contratos que garantam que as referidas instituições tomem medidas e precauções para corretamente identificar os Investidores e a origem de seus recursos.

Assim, os contratos celebrados entre a Gestora e referidos administradores fiduciários e distribuidores deverão contemplar obrigações que lhes exijam (i) efetuar a devida identificação de clientes mediante preenchimento de cadastros completos e procedimentos que garantam a manutenção de tais cadastros devidamente atualizados, (ii) adotar rotinas e processos que lhes permitam possuir o necessário conhecimento dos Investidores (KYC), evitando-se o uso da conta por terceiros e identificando-se os beneficiários finais das operações, e (iii) a aplicação de metodologias e sistemas que confrontem as informações cadastrais com as movimentações praticadas por referidos Investidores com vistas a detectar quaisquer indícios de lavagem de dinheiro. A aceitação de novos Investidores e o monitoramento de transações praticadas pelos Investidores deverão estar amparados em critérios que levem em conta a localização geográfica do Investidor, o tipo de atividade/profissão do cliente em questão e os produtos por estes escolhidos para investimento.

Neste sentido, os administradores fiduciários e distribuidores dos Veículos de Investimento devem, dentre outras obrigações: (i) adotar regras contínuas, procedimentos e controles internos para confirmar as informações de registro dos Investidores, mantendo tais registros devidamente atualizados; (ii) monitorar as transações realizadas pelos Investidores com a finalidade de evitar o uso da conta por terceiros; (iii) identificar os beneficiários finais das operações (adotando políticas de KYC); (iv) identificar as pessoas consideradas politicamente expostas[3] ("PEPs"), mantendo regras, procedimentos e controles internos que identifiquem Investidores que se tornem PEPs e a fonte dos fundos envolvidos nas transações de Investidores e beneficiários identificados como PEPs; (v) supervisionar rigorosamente a

[3] Para os fins da Instrução CVM 301, uma PEP é uma pessoa que desempenha ou tenha desempenhado, nos últimos 5 anos, posições públicas relevantes, trabalhos ou funções, no Brasil ou outros países, territórios e dependências estrangeiras, bem como, seus representantes, parentes e outras pessoas relacionadas a eles. Além disso, a Instrução CVM 301 também define como PEP: (i) os titulares de mandatos eleitos dos poderes executivos e judiciários federais; (ii) os titulares de determinadas posições no poder executivo federal; (iii) os membros do Conselho de Justiça Nacional, o Supremo Tribunal Federal e os tribunais superiores; (iv) os membros do Conselho Nacional do Ministério Público, a Procuradoria Geral da República, a Procuradoria Geral Adjunta da República, a Procuradoria Geral do Trabalho, a Procuradoria Geral da Justiça Militar, a Procuradoria Geral Adjunta da República e a Procuradoria Geral da Justiça dos Estados e Distrito Federal; (v) os membros do Tribunal de Auditoria Federal e Procuradoria Geral do Ministério Público para o Tribunal de Auditoria Federal; (vi) os Governadores do Distrito do Estado e Federal, os Presidentes do Tribunal de Justiça, Assembleia Legislativa e o Conselho Distrital e Presidente do Tribunal e Conselho de Contas dos Estados, Municipalidades e Distrito Federal; e (vii) os Prefeitos e Presidentes do Conselho Municipal das capitais do Estado.

relação comercial mantida com as PEPs, dedicando especial atenção às propostas de iniciação de relação e as operações executadas com PEPs; e (vi) supervisionar rigorosamente as operações com Investidores estrangeiros, especialmente quando organizados sob a forma de *trusts* ou sociedades com títulos ao portador, bem como operações com Investidores de private banking.

Os administradores fiduciários e distribuidores dos Veículos de Investimento, conforme o caso, devem dedicar especial atenção a algumas categorias de operações, tais como operações cujos valores sejam inadequados com a ocupação profissional, os ganhos e/ou situação financeira do Investidor, operações que representem uma oscilação significativa com relação ao volume e/ou frequência de negócios usualmente realizados por tal Investidor, operações executadas buscando gerar perdas ou ganhos sem base econômica objetiva, operações com a participação de pessoas físicas residentes ou entidades constituídas em países que não aplicam as recomendações da Força-Tarefa de Ação Financeira contra Lavagem de Dinheiro e Financiamento Terrorista – FATF, operações cujo nível de complexidade e risco são inadequados à qualificação técnica do Investidor ou situações em que não é possível manter as informações atualizadas de registro do Investidor ou identificar o beneficiário final.

A Gestora, por sua vez, diligenciará junto a tais administradores fiduciários e distribuidores dos Veículos de Investimento, sempre que o(a) Diretor(a) de Risco e *Compliance* entenda necessário (mas em periodicidade nunca inferior a uma visita de *due diligence* anual) para assegurar que referidos prestadores de serviço possuem os recursos humanos, ferramentas de TI (em especial, sistemas de AML que lhe permitam confrontar as informações de Investidores com as operações de forma automatizada e em tempo real) e adotam processos e rotinas que lhes permitam a devida condução dos procedimentos pertinentes à prevenção contra lavagem de dinheiro previstos neste Manual.

Caso a revisão periódica de quaisquer desses prestadores de serviços não seja satisfatória, a critério do(a) Diretor(a) de Risco e *Compliance*, deverá este imediatamente comunicar o Comitê de Risco e *Compliance* e diligenciar para que o prestador em questão desenvolva o serviço de forma adequada ou seja prontamente substituído por um novo prestador.

Importante ressaltar que a Gestora não atua como gestora de carteiras administradas no Brasil, gerindo exclusivamente fundos de investimento para os quais não presta serviços de

administração e/ou distribuição de cotas. Não obstante, a Gestora diligencia ativamente perante os terceiros indicados nos parágrafos acima - que são efetivamente as instituições que mantêm relacionamento direto com os Investidores – para assegurar que a política prevista neste Manual está sendo cumprida.

Caso a Gestora identifique a ocorrência de quaisquer transações, ou propostas de transação, que possam constituir indicações sérias de crimes referentes à "lavagem" ou ocultação de ativos, direitos e objetos de valor derivados de infrações penais, nos termos da Lei 9.613/98, comunicará o Conselho de Controle de Atividades Financeiras - COAF, dentro do prazo de 24 horas de sua ocorrência. O(A) Diretor(a) de Risco e *Compliance* possui soberania e autonomia para comunicação de indícios da ocorrência dos crimes previstos na Lei 9.613 ou a eles relacionados.

1.3.2. Monitoramento de Investimentos realizados pelos Veículos de Investimento (Ativo)

Sob a ótica de monitoramento dos investimentos realizados por seus Veículos de Investimento, a Gestora é a responsável pelo processo de identificação da contraparte das operações de investimento, visando prevenir que referidas contrapartes utilizem a Gestora ou seus Veículos de Investimento para atividades ilegais ou impróprias.

Neste sentido, a Gestora, na qualidade de instituição gestora dos Veículos de Investimento, adota as seguintes medidas com vistas a inibir práticas atreladas à lavagem de dinheiro por intermédio dos Veículos de Investimento:

- Formalização nos mandatos de seus Veículos de Investimento (i.e. mediante inserção expressa neste sentido nos regulamentos dos Fundos CVM e *offering* memoranda de Fundos *Offshore*) de vedação completa à realização de operações de *day-trade* pelos Veículos de Investimento;

- Os Veículos geridos pela Gestora em sua maioria investem em outros fundos geridos por terceiros e uma parte relevante do processo de Due Diligence para a seleção de gestores é a revisão dos documentos de *Compliance* da gestora, para que esteja em dia com as políticas do órgão regulador pertinente, uma Diligência operacional para verificar as práticas operacionais bem como para conhecer as pessoas responsáveis por Operações e por *Compliance*, e também verificar as contrapartes do fundo no qual

estaremos investindo, bem como os provedores de serviço de custódia e administração;

- Investimentos feitos em ativos diretos pelos Veículos de Investimento da Gestora são feitos com um número limitado de contrapartes, todas de renome, e nenhuma operação é feita para *day-trade*; e

- Vedação à realização de transações entre os Fundos CVM geridos pela Gestora, e nos Fundos *Offshore* mediante à anuência do administrador fiduciário internacional. Em função do fato de que os poucos ativos e valores mobiliários negociados diretamente pelos Veículos de Investimento terem por contraparte instituições financeiras e equiparadas de primeira linha, a Gestora, com respaldo no quanto previsto no "*Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro*" publicado pela ANBIMA, entende que os procedimentos e controles internos elencados no presente Manual são adequados e garantem o atendimento aos padrões mínimos de combate à lavagem de dinheiro exigidos pelas normas em vigor, sendo dispensada, neste momento, a adoção de procedimentos ou controles adicionais.

Caso, no entanto, a Gestora altere a estratégia de investimento dos seus Veículos de Investimento de modo a contemplar títulos e valores mobiliários objeto de distribuição privada, direitos creditórios, empreendimentos imobiliários, etc, deverá o(a) Diretor(a) de Risco e *Compliance* previamente adequar a política da Gestora com vistas a contemplar procedimentos que permitam o devido controle e monitoramento das contrapartes e faixas de preços dos ativos negociados em nome dos Veículos de Investimento sob sua gestão.

Por fim, caso a Gestora identifique a ocorrência de quaisquer transações praticadas pelos Veículos de Investimento ou propostas de transações que possam constituir indicações sérias de crimes referentes à "lavagem" ou ocultação de ativos, direitos e objetos de valor derivados de infrações penais, nos termos da Lei 9.613/98, comunicará o Conselho de Controle de Atividades Financeiras - COAF, dentro do prazo de 24 horas de sua ocorrência. O(A) Diretor(a) de Risco e *Compliance* possui soberania e autonomia para comunicação de indícios da ocorrência dos crimes previstos na Lei 9.613 ou a eles relacionados.

1.3.2.1 Processo de identificação de Contrapartes (Cadastro)

Caso venha a se aplicar, a M Square irá estabelecer processo de identificação de contraparte adequado às características e especificidades dos seus negócios, conforme abaixo descrito. Os ativos e valores mobiliários elencados abaixo, em função de sua contraparte e do mercado nos quais são negociados, já passaram pelo processo de prevenção à Lavagem de Dinheiro, eximindo, portanto, a M Square de diligência adicional em relação ao controle da contraparte, a saber:

- Ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM;
- Ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;
- Ativos e valores mobiliários admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida;
- Ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e
- Ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (a) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

1.3.2.2 Ações Negociadas em Bolsa – Baixa Liquidez

Como exceção ao acima disposto, e de acordo com as recomendações do Ofício-Circular CVM/SIN/N. 5/2015, caso a M Square adquira diretamente ações em bolsa de baixa liquidez dispensará especial atenção às operações suspeitas e passiveis de serem reportadas ao COAF nos casos de negociações realizadas em bolsa de valores em que seja possível, considerando circunstancias próprias da negociação, determinar a contraparte dos

negócios, como por exemplo quando da negociação de ativos de liquidez muito baixa ou quando se tratar de uma operação entre os Fundos CVM.

1.3.2.3 Crédito Privado, Operações em Balcão Organizado e Distribuição Privada

Embora atualmente adquiram apenas cotas de outros fundos de investimentos, eventualmente, os Fundos CVM poderão adquirir, como parte de sua estratégia, derivativos de balcão ou ativos de crédito privado, no Brasil ou no exterior. Nesses casos, a M Square tem como regra geral atuar com contraparte que sejam instituições financeiras ou equiparadas, brasileiras ou estrangeiras.

Atualmente, os Fundos buscam negociar estes tipos de ativos apenas através de outros fundos geridos por terceiros, razão pela qual a regulamentação de crédito privado não se aplica atualmente em sua essência à M Square (constituição através de cessão de crédito, garantia e monitoramentos).

A M Square não tem como política adquirir ativos através de distribuição privada (renda fixa ou ações), nem tampouco direitos creditórios e empreendimentos imobiliários.

Porém nos casos em que a contraparte da operação não for uma instituição financeira ou equiparada, ou não constar de nenhum dos itens de exceções mencionados acima, a M Square deverá adotar processo de identificação de contrapartes, bem como monitorar eventual direcionamento de ganhos ou perdas, ou ainda a existência de outros indícios de Lavagem de Dinheiro, inclusive verificando, quando for o caso, se a contraparte dispõe de mecanismos mínimos para tal análise.

1.3.2.4 Procedimento de Cadastro de Contrapartes

Quando aplicável, o cadastro das contrapartes com quem a Gestora faça negócios deverá ser padronizado, mediante o preenchimento, pela respectiva contraparte, do formulário que constitui o **Anexo A** à presente. A área de *Compliance*, a seu exclusivo critério, poderá dispensar o preenchimento de determinados itens do referido formulário. Os documentos relativos ao cadastro da contraparte deverão ser arquivados pelo prazo mínimo de 5 (cinco) anos.

1.3.2.5 Operações Diretas

Se e quando existentes, as operações "diretas" realizadas pelos Fundos CVM deverão seguir as Políticas de Decisão de Investimentos e de Seleção e Alocação de Ativos e de Rateio e Divisão de Ordens, que constituem os Anexos V e VI do Manual de *Compliance*, respectivamente, cujo propósito principal é o rebalanceamento de posições entre Fundos CVM geridos de forma *pari passu*, sempre em mercado ou mediante utilização de instituição financeira como contraparte, não sendo política da M Square realizar operações diretas entre os Fundos CVM fora desses ambientes.

Qualquer operação "direta" efetuada pela M Square que fuja deste propósito, seja entre os Fundos CVM ou tendo terceiros como contraparte final, constitui exceção e deverá ser aprovada pelo Comitê de Investimentos.

A área de *Compliance* deverá monitorar continuamente os procedimentos de exceções e todas as operações diretas.

1.3.2.6 Monitoramento de Situações Atípicas e Comunicação ao COAF

Por meio dos mecanismos de controles estabelecidos nesta Política, será realizado o monitoramento das operações e situações previstas no art. 6º da Instrução CVM nº 301/99, em especial de operações realizadas com finalidade de gerar perda ou ganho, para as quais falte, objetivamente, fundamento econômico.

Para tanto, na execução de operações por conta e ordem dos Veículos de Investimento, a equipe de gestão deverá dispensar especial atenção e exercer todos os esforços para se certificar que a operação (i) é legítima, e ocorre de acordo com as características normais de mercado, no que se refere às partes envolvidas, forma de realização ou instrumentos utilizados; (ii) em fundamento econômico determinável e não obscuro; e (iii) dispensar esforços para identificação da contraparte, conforme acima.

Qualquer operação que fuja aos preceitos acima não deverá ser realizada e a ocorrência deve ser imediatamente comunicada à área de *Compliance*.

Nesses casos, o(a) Diretor(a) de Risco e *Compliance* deverá avaliar a necessidade de comunicação ao COAF, levando o caso para apreciação do Comitê de Risco e *Compliance*, a quem caberá a decisão final pela necessidade de comunicação.

Caso a Gestora não tenha prestado nenhuma comunicação de operação suspeita ao COAF em determinado ano civil, a área de *Compliance* deverá realizar comunicação negativa, pelo SISCOAF, até o fim de janeiro do ano subsequente.

1.4. Designação de Diretora Responsável por AML

O(A) Diretor(a) de Risco e *Compliance* será a responsável pelo cumprimento das normas relativas à prevenção contra lavagem de dinheiro e por fornecer as orientações para os Colaboradores e a Companhia visando assegurar que políticas e medidas anti-lavagem de dinheiro previstas neste Manual estão sendo efetivamente aplicadas, inclusive por administradores fiduciários e distribuidores dos Veículos de Investimento, de forma a resguardar a Gestora de quaisquer ameaças ou consequências relativas à lavagem de dinheiro.

Tais medidas incluem: (i) a revisão do processo de *due diligence* e atualizações realizadas pelos administradores e distribuidores com relação a novos Investidores e Investidores existentes, em observâncias às normas de "Conheça seu Cliente" (*Know Your Client*), (ii) assegurar-se da implementação de sistemas por administradores fiduciários e distribuidores para a efetiva identificação, monitoramento e reporte de transações suspeitas, (iii) assegurar-se que administradores fiduciários e distribuidores realizem continuamente programas de treinamento para seus colaboradores, envolvendo ao menos uma introdução à regulamentação e recomendações quanto à lavagem de dinheiro, definição de tais atividades e seus desenvolvimentos recentes, (iv) avaliação dos procedimentos de reporte adotados por administradores fiduciários e distribuidores, (v) revisão e verificação de quaisquer outras medidas anti-lavagem de dinheiro da companhia, dos administradores fiduciários e distribuidores em intervalos periódicos, bem como sugestão de introdução de novas medidas, substituição ou modificação de medidas antiquadas, sempre que julgar necessário no seu melhor entendimento, (vi) manter-se atualizada quanto às mudanças na regulamentação nacional e internacional relativa à lavagem de dinheiro, e (vii) condução de treinamentos para os Colaboradores da Gestora em intervalos periódicos no mínimo anuais.

ANEXO A

QUESTIONÁRIO DE *DUE DILIGENCE* - PLD DA M SQUARE

[NOME DO ADMINISTRADOR / DISTRIBUIDOR /CONTRAPARTE/EMISSOR]

Em nome da M Square Investimentos Ltda. ("M Square"), encaminho este documento com o fim de cadastrar as informações acerca dos controles internos de prevenção à lavagem de dinheiro adotas pela Gestora.

Contamos com a colaboração de V.Sas. e solicitamos que as informações sejam verdadeiras, confiáveis e íntegras.

A M Square assegura que todas as informações aqui prestadas serão mantidas internamente e não serão disponibilizadas a terceiros, salvo se solicitado por autoridades públicas competentes ou medidas judiciais.

Periodicamente, a M Square poderá solicitar a revisão deste questionário.

Ao final do questionário, favor indicar o responsável pelo preenchimento deste e, se houver mais do que um, ambos devem ser identificados.

Atenciosamente,

M Square Investimentos Ltda.

m square

Informações Cadastrais

1.1. - Razão Social:

1.2. - CNPJ/MF:

1.3. - Endereço:

1.4. - Principais contatos:

E-mails:

Telefones:

Celulares:

1.5. – Registros em órgãos reguladores, autorreguladores e associações de classe:

1.6. – Pertence a algum grupo financeiro? Qual(is)?

---

2. Informações sobre os controles da Política de Lavagem de Dinheiro e Financiamento ao Terrorismo:

2.1. A Instituição possui Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo?

( ) Sim. Favor anexar.

( ) Não.

2.2. A Instituição possui procedimento de identificação e registro dos investidores ("Conheça seu Cliente")?

( ) Sim. Favor anexar.

( ) Não.

2.3. Os controles e procedimentos de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo são submetidos à auditoria externa? Qual a periodicidade?

( ) Sim. Periodicidade? _____

( ) Não.

2.4. A Instituição está submetida à quais normas de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (legais, regulatórias e autorregulatórias)?

2.5. Quantas pessoas estão alocadas na área de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo? Existem sistemas de controle?

2.6. A Instituição, seus sócios, diretores ou qualquer outro funcionário possui algum relacionamento com pessoas consideradas politicamente expostas*?

( ) Sim. Detalhar:

( ) Não.

*Consideram-se pessoas politicamente expostas os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

2.7. A Instituição, sócios ou diretores já foram acusados na esfera administrativa ou criminal ou condenados por crimes de (i) lavagem de dinheiro, (ii) contra o patrimônio, ou (iii) contra o sistema financeiro nacional ou ainda por qualquer outro crime?

2.7. Favor informar o nome da Diretora responsável pela Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo.

Data: Nome: Assinatura do responsável:

ANEXO II

POLÍTICA DE CONTROLES INTERNOS E DE *COMPLIANCE*

1 Objetivo

A área de *Compliance* da M Square é responsável pela elaboração e manutenção do Programa de *Compliance* da Gestora, que inclui a revisão e atualização periódica das Políticas constantes deste Manual e demais políticas e procedimentos internos, bem como a implementação de controles internos e testes de aderência para monitorar a efetividade das mesmas e, ainda, a realização de treinamentos aos Colaboradores.

O Programa de *Compliance* da Gestora foi desenvolvido com vistas a dar cumprimento às obrigações estabelecidas na Instrução CVM nº 558/15, conforme alterada ("Instrução CVM 558"), nos Códigos de autorregulação da ANBIMA dos quais a M Square seja aderente ou deva observar, bem como demais normas, diretrizes e Ofícios de Orientação emitidos pelos referidos órgãos, dentre outras melhores práticas nacionais e internacionais aplicáveis às atividades da M Square.

A área de *Compliance*, com apoio do Comitê de Risco e *Compliance*, é a principal responsável pela disseminação e supervisão das regras, controles e procedimentos internos da Gestora, visando mitigar os riscos operacionais, regulatórios, reputacionais e legais de suas atividades. Para tanto, a área conta dois profissionais, capacitados com a qualificação técnica e experiência necessárias para sua função, e sistemas definidos nesta política.

A Gestora utiliza o sistema denominado Compli.ly, para gestão de *Compliance*. Tal sistema disponibiliza uma agenda de atividades regulatórias atualizada, controles internos e testes de aderência para cumprimento das normas de regulação e autorregulação aplicáveis à Gestora. O sistema possui, ainda, uma biblioteca digital para armazenamento de documentos e registro de eventos. Portanto, os registros e arquivamentos a cargo da área de *Compliance* poderão ser realizados no referido sistema, a critério da área de *Compliance*. Além disso, todas as atividades, eventos e demais registros imputados no referido sistema possuem logs de registro para fins de auditoria e backups automáticos.

Esta política objetiva, portanto, disciplinar a atuação da área de *Compliance* da M Square, esclarecendo suas responsabilidades e os procedimentos a serem observados quando de sua atuação, e estará disponível a todos os Colaboradores, na intranet / Website da Gestora.

2 Diretor(a) de Risco e *Compliance*

O(A) Diretor(a) responsável por *Compliance* e gestão de riscos encontra-se nomeada no contrato social da M Square ("Diretor(a) de Risco e *Compliance*"), sendo assim, nos termos do art. 22 da Instrução CVM 558, responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos na referida instrução e na autorregulação da ANBIMA.

Reportando-se diretamente ao Comitê de Risco e *Compliance*, tem plena autoridade sobre a implementação do Programa de *Compliance* da Gestora, e possui experiência com a legislação e regulamentação do mercado de capitais.

O(A) Diretor(a) de Risco e *Compliance* é uma das administradoras / representantes legais da Gestora, na forma do seu contrato social. Ademais, a parte mais substancial de sua remuneração é garantida, de forma totalmente independente da performance dos fundos, como mais uma maneira de garantir sua independência. O mesmo ocorre com os demais recursos humanos que integram as áreas de Risco e *Compliance* da M Square no que tange à forma de remuneração.

São obrigações do(a) Diretor(a) de Risco e *Compliance*, no âmbito desta política:

a. Atender prontamente todos os Colaboradores;

b. Identificar possíveis condutas contrárias à lei, regulação, autorregulação, políticas e manuais da Gestora; e

c. Tomar as decisões acerca das infrações cometidas, quando aplicável.

Todo e qualquer Colaborador da M Square que souber de informações ou situações em andamento, que possam afetar os interesses da Gestora, gerar conflitos ou, ainda, se revelarem contrárias aos termos previstos nesta política, deverá informar o(a) Diretor(a) de Risco e *Compliance*, para que sejam tomadas as providências cabíveis.

Ainda, cabe a(o) Diretor(a) de Risco e *Compliance* analisar situações que possam ser caracterizadas como "conflitos de interesse" pessoais e profissionais.

3 Comitê de risco e *Compliance*

O Comitê de Risco e *Compliance* se reunirá no mínimo semestralmente, ou sempre que necessário, mediante convocação por e-mail do(a) Diretor(a) de Risco e *Compliance,* nas reuniões ordinárias, ou de qualquer de seus membros, nos demais casos. O Comitê de Risco e *Compliance* deverá ser instalado necessariamente com a presença do Coordenador ou, na sua ausência, seu suplente.

O Comitê de Risco e *Compliance* terá plena autonomia para o exercício de suas funções. O Comitê será composto por: (i) Diretor(a) de Risco e *Compliance*, (ii) ao menos 1 (um) membro dos seus departamentos técnicos dedicados às áreas de *Compliance* e gestão de riscos; e (iii) o(a) Diretor(a) de Investimentos, observado o mecanismo de impedimento ao voto no caso de conflito de interesses relativamente às áreas de sua supervisão direta ou si própria.

A coordenação direta do Comitê de Risco e *Compliance* ficará a cargo do(a) Diretor(a) de Risco e *Compliance*, o qual terá o voto de "minerva"[4] no caso de empate nas deliberações do Comitê. Cabe a(o) Diretor(a) de Risco e *Compliance* arguir o impedimento ao direito de voto do(a) Diretor(a) de Investimentos e/ou de algum membro do Departamento Comercial, caso os mesmos não o façam, visando evitar conflito de interesses.

O(A) Diretor(a) de Risco e *Compliance* poderá delegar determinadas funções para outros Colaboradores que entenda ser qualificado para tanto, desde que tais funções continuem sob sua imediata supervisão. Dessa forma, qualquer referência aos deveres do(a) Diretor(a) de Risco e *Compliance* aqui previstos, incluirá os de pessoa por este designada.

O Comitê de Risco e *Compliance* arquivará em sistema eletrônico ou arquivo físico todos os materiais de trabalho que servem de apoio para fundamentar as suas discussões e decisões aprovadas nas respectivas reuniões do Comitê pelo prazo mínimo de 5 (cinco) anos.

3.1 Deveres e Responsabilidades do Comitê de Risco e *Compliance*

São deveres e responsabilidades do Comitê de Risco e *Compliance*, além das previstas na Política de Gestão de Riscos da Gestora:

[4] Voto de Minerva é o que decide uma votação que de outra forma estaria empatada.

- Definir, divulgar e revisar os procedimentos contidos nesta Política, bem como as demais políticas aplicáveis à Gestora, devendo aprovar quaisquer alterações nestas;
- Avaliar todos os casos que cheguem ao seu conhecimento sobre o descumprimento das diretrizes previstas nesta política ou nas demais políticas da Gestora, e também apreciar e analisar situações não previstas nos referidos documentos;
- Tratar todos os assuntos que cheguem ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da Gestora, garantindo o sigilo de eventuais denunciantes de delitos ou infrações, exceto nos casos de necessidade de testemunho judicial;
- Solicitar, sempre que necessário, o apoio de terceiros especializados, tais como advogados, consultorias, ou auditoria externa;
- Definir os princípios éticos a serem observados por todos os Colaboradores, constantes das políticas internas da Gestora, e promover a ampla divulgação e aplicação dos preceitos éticos de *Compliance* no desenvolvimento das atividades da Gestora;
- Deliberar sobre situações que possam ser caracterizadas como conflitos de interesse tanto pessoais como profissionais. Esses conflitos podem acontecer, inclusive, mas não se limitando, às seguintes situações endereçadas em políticas próprias: investimentos pessoais, atividades externas, presentes e entretenimentos, contribuições políticas, transações com partes relacionadas, alocações de oportunidades e despesas entre veículos geridos, dentre outros exemplos;
- Apurar e tomar determinadas decisões e aprovações de Risco, *Compliance*, Prevenção à Lavagem de Dinheiro e Não Financiamento do Terrorismo, Anticorrupção e Plano de Contingências;
- Apurar denúncias ou indícios de condutas potencialmente contrárias às Políticas internas e normas legais ou regulatórias, avaliando a necessidade de comunicação aos órgãos reguladores ou COAF, e ainda avaliar e discutir sanções internas;Fornecer orientação aos Colaboradores em caso de dúvidas quanto à aplicação das Políticas da M Square, que não puderem ser esclarecidas diretamente pela área de *Compliance*;
- Coordenar quaisquer fiscalizações regulatórias, sejam estas conduzidas pela CVM ou ANBIMA;

- Aprovar o oferecimento de novos produtos e serviços, incluindo novas estratégias de investimentos, e tipos de fundos geridos, bem como a modificação de condições relevantes dos produtos ofertados;
- Aprovar o relacionamento com determinados Investidores que envolvam grau de risco; e
- Monitorar o desempenho dos Colaboradores em seu ambiente de trabalho, a fim de identificar possíveis condutas contrárias às políticas e manuais da Gestora e legislação aplicável.

4 ÁREA DE *COMPLIANCE*

4.1 Funções e Responsabilidades da Área de *Compliance*

As seguintes atividades são de responsabilidade primária da área de *Compliance*:

- Anualmente e nos casos de revisão, fornecer uma cópia do Manual de *Compliance* e demais políticas relevantes da Gestora para cada Colaborador;
- Obter de cada Colaborador as declarações e divulgações de informações requeridas segundo os vários anexos do Manual de *Compliance* e demais políticas relevantes da Gestora;
- Revisar os controles de riscos de mercado, liquidez, concentração, contraparte, operacional e de crédito, inerente aos Fundos CVM, conforme disposto na Política de Gestão de Riscos da M Square, observando integralmente as diretrizes do art. 23 da Instrução CVM 558 e do Código ANBIMA e das melhores práticas determinadas pela ANBIMA, através da implementação de testes periódicos;
- Coordenar com os sócios e assessores jurídicos da Gestora eventuais revisões das questões de *Compliance* e avaliar o impacto das alterações relevantes nas leis e normas aplicáveis;
- Prontamente atender todos os Colaboradores em relação a dúvidas sobre *Compliance*
- Fornecer aconselhamento e suporte consultivo às áreas de negócios, Comitês internos e à Diretoria a respeito de regras e normas emanadas de órgãos reguladores e autorreguladores;
- Gerir o Código de Ética e Conduta, zelando pela manutenção do dever fiduciário perante os Fundos e Investidores, prevendo e implementando procedimentos para mitigação de eventuais conflitos de interesse, bem como zelando pela observância das vedações normativas previstas no art. 16 da Instrução CVM 558;

- Implementar Programas de Treinamento dos Colaboradores, conforme definido no item 5 desta política, incluindo mas não se limitando àqueles destinados aos Colaboradores que têm acesso a informações confidenciais da Gestora, e seus clientes e investidores, bem como treinamentos específicos para a Área de *Compliance*, dentre outros;
- Identificar, documentar e avaliar os riscos associados à conformidade da atividade da Gestora aos preceitos normativos, analisando o impacto do oferecimento de novos produtos e serviços ou de relacionamento com determinados Investidores que envolvam grau de risco;
- Manter os formulários regulatórios, em especial o Formulário de Referência, responsabilizando-se pela atualização e revisão periódica destes documentos, inclusive mantendo as informações atualizadas no *website* da Gestora e com à CVM e a ANBIMA;
- Realizar acompanhamento das principais normas, diretrizes e alertas emanados de órgãos reguladores e autorreguladores e manter atualizada a agenda regulatória contendo todos os prazos emanados de tais órgãos, podendo usar sistemas eletrônicos para tanto;
- Realizar testes periódicos a fim de monitorar e avaliar a efetividade do Programa de *Compliance* da M Square, suas políticas e procedimentos e dos sistemas e controles da Gestora, sugerindo e acompanhando as ações de melhorias decorrentes de tais testes, podendo utilizar-se de sistema eletrônico próprio para tanto e sempre manter evidências dos testes realizados;
- Realizar testes de controles de acesso em recursos computacionais (diretórios internos e sistemas), bem como outros testes para verificação das funcionalidades dos sistemas eletrônicos utilizados pela Gestora e disponibilização efetiva de *backups* dos documentos e sistemas.
- Desenvolver um relatório de controles internos conforme estabelecido no art. 22 da Instrução CVM 558, o qual deverá ser elaborado anualmente e disponibilizado ao Comitê de Risco e *Compliance* e para os Diretores, até o último dia útil do mês de abril, relativo ao ano civil imediatamente anterior à data de entrega (com base nos testes de aderência referidos no item acima);
- Manter atualizadas e disponíveis no *website* da Gestora as políticas previstas no art. 14 da Instrução CVM 558, constantes desta Política, bem como aquelas cuja publicidade seja exigida pela ANBIMA;

- Providenciar atendimento a fiscalizações e supervisões de órgãos reguladores e autorreguladores, auditorias terceirizadas e *due dilligences*, fazendo a interface entre as solicitações destes e as áreas internas da M Square;
- Gerir as Atividades de Prevenção à Lavagem de Dinheiro e Não Financiamento do Terrorismo, implementando a política própria e seus procedimentos de forma a mitigar a ocorrência de situações atípicas e permitindo sua imediata identificação na ocorrência e eventual comunicação ao COAF;
- Estabelecer o padrão e aprovar os materiais de comunicação e marketing, conforme procedimento estabelecido na política própria, tendo por base o Código ANBIMA e outras Diretrizes da ANBIMA que sejam aplicáveis;
- *Cross border issues*: avaliar questões regulatórias aplicáveis nas jurisdições estrangeiras com as quais a M Square realize operações ou tenha registro;
- Gerir as Políticas de Atividades Externas e de Investimentos Pessoais de Colaboradores, incluindo a concessão de aprovações quando for o caso, e monitoramentos periódicos;
- Informar à CVM sempre que verifique, no exercício das suas atribuições, a ocorrência ou indícios de violação da legislação que incumbe à CVM fiscalizar, no prazo máximo de 10 (dez) dias úteis da ocorrência ou identificação;
- Realizar monitoramento de e-mails corporativos de Colaboradores sempre que julgar necessário;
- Verificar, no mínimo anualmente, se os "Colaboradores-chave", em especial os sócios controladores e os Sócios Diretores, estão envolvidos em processos administrativos de órgão reguladores e autorreguladores, criminais de qualquer natureza, ou ainda outros processos que possam trazer contingências para a Gestora e que, portanto, sua divulgação pública possa vir a ser necessária, nos termos da Instrução CVM nº 558/15;
- Verificar se os devidos profissionais da área de Gestão estão com sua certificação ou isenção vigentes, manter a Base de Dados da ANBIMA atualizada, bem como verificar se os demais procedimentos das Políticas de Certificação Continuada de Colaboradores e de Seleção e Contratação de Colaboradores estão sendo cumpridos;
- Confirmar, por meio do CVMWEB, até o dia 31 de março de cada ano, que as informações contidas no formulário cadastral da Gestora previsto na Instrução CVM nº 510/11 continuam válidas, bem como atualizar o referido formulário cadastral sempre que qualquer dos dados

neles contido for alterado, em até 7 (sete) dias úteis contados do fato que deu causa à alteração; e

- Realizar quaisquer outras atividades, monitoramentos, testes ou controles internos que lhe sejam expressamente atribuídas por esta política ou outras políticas da M Square.

Sempre que entender necessário ou conveniente, o(a) Diretor(a) de Risco e *Compliance* poderá levar qualquer assunto de sua competência para apreciação ou deliberação pelo Comitê de Risco e *Compliance*.

5 Treinamento de *Compliance*

Todos os Colaboradores, inclusive da própria área de *Compliance*, comparecerão a uma "**Reunião Anual de Treinamento de *Compliance***" e, sempre que a área de *Compliance* julgar necessário, reuniões adicionais sobre o tema, em razão de alterações normativas, regulatórias ou da própria atividade da Gestora.

A necessidade de treinamento adicional para novos Colaboradores fica a cargo da área de *Compliance*, que dependendo de suas funções nos termos desta política, deverá ministrá-lo tão logo inicie suas atividades na M Square. Este treinamento levará em conta as mudanças no mercado, produtos, legislação e regulamentação, bem como a avaliação de sua aplicação de conhecimento.

A Reunião Anual de Treinamento de *Compliance* cobrirá, no mínimo:

- Uma revisão da infraestrutura de *Compliance* da Gestora, se necessário;
- Uma revisão sobre as regras de Anticorrupção e procedimentos internos correlatos;
- Uma revisão das principais regras e premissas desta política e do Código de Ética;
- Uma sessão de perguntas e respostas durante a qual os Colaboradores poderão tirar dúvidas e receber orientação sobre as questões de *Compliance*; e
- Uma revisão dos desenvolvimentos regulatórios recentes, bem como de quaisquer alterações nas linhas de negócios da Gestora.

O(A) Diretor(a) de Risco e *Compliance* elaborará e distribuirá uma agenda da Reunião e manterá um controle de presença assinado por todos os Colaboradores presentes.

6 Revisão anual de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* realizará não menos do que uma revisão anual de adequação das políticas e procedimentos da Gestora e eficácia de sua implantação, devendo elaborar o Relatório

de Controles Internos, nos termos do art. 22 da Instrução CVM 558. O(A) Diretor(a) de Risco e *Compliance* revisará o Manual e demais políticas para garantir que permaneça consistente com as atividades da Gestora e desenvolvimentos regulatórios relevantes ou contratar terceiros especializados para tanto.

7 Registro e reporte de gestor de recursos de terceiros

7.1 Processo de Registro do Gestor de Recursos de Terceiros no Brasil

Para se registrar como um gestor de recursos de terceiros perante a CVM, o gestor deve submeter um requerimento à CVM, de acordo com a Instrução CVM 558. Como é o caso da M Square, para manter-se registrado, dentre outras obrigações, a Gestora deverá cumprir com as obrigações de envio de informações e formulários, descritos na Política de Controles Internos e de *Compliance* deste Manual.

7.1.1 Exigências e Procedimentos de Registro

De acordo com a Instrução CVM 558, a autorização para exercer a atividade de gestão de carteira de valores mobiliários no Brasil somente será concedida a uma entidade legal domiciliada no Brasil que: (i) descreva em seu objeto social os serviços de gestão de carteira de valores mobiliários; (ii) seja devidamente constituída e registrada junto ao CNPJ (Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda); (iii) atribua a responsabilidade pela atividade de gestão de carteira de valores mobiliários a um diretor estatutário autorizado pela CVM para exercer essa atividade; (iv) atribua a responsabilidade por *Compliance* e gestão de riscos a um diretor estatutário; (v) constitua e mantenha recursos humanos e computacionais adequados ao seu porte, entre outros.

O(A) Diretor(a) responsável pela atividade de gestão de Fundos CVM, autorizada pela CVM ao exercício de referida função, encontra-se nomeada no contrato social da M Square ("Diretor(a) de Investimentos").

Como mencionado acima, o(a) Diretor(a) de Risco e *Compliance* também se encontra nomeado no contrato social da M Square.

A solicitação da autorização para exercer atividades de administração de carteira de valores mobiliários, apresentada por uma entidade legal, deve incluir, sem limitação a outros documentos e informações: (i) cópia dos atos de constituição, em sua versão vigente e

atualizada, devendo conter a indicação dos diretores responsáveis pela gestão de Veículos de Investimento e por *Compliance* e gestão de riscos; e (ii) informação a respeito da Gestora e seu grupo econômico, recursos humanos, estrutura operacional e administrativa.

Além disso, a Gestora deverá preparar e manter versões atualizadas deste Manual, do Código de Ética em seu website, juntamente com os seguintes documentos: (i) Formulário de Referência, cujo conteúdo deve refletir o Anexo 15-II da Instrução CVM 558; (ii) Política de Gestão de Risco; (iii) Política de compra e venda de valores mobiliários por empregados, colaboradores e pela própria Gestora; e (iv) Política de rateio e divisão de ordens entre os Veículos de Investimento (conforme Anexo VI do Manual de *Compliance*).

A autorização para exercer a atividade de administração de carteira de valores mobiliários é concedida por meio de um Ato Declaratório.

7.1.2 Fiscalizações da CVM

Após a autorização para exercer as atividades de administração de carteira de valores mobiliários, a CVM poderá conduzir, em qualquer momento, fiscalizações ou investigações na sede do gestor. O poder de fiscalização da CVM incide sobre todos os registros de um gestor de recursos de terceiros. Conforme julgue necessário, a CVM poderá iniciar um processo administrativo para investigar as violações regulatórias e aplicar penalidades.

7.1.3 Aplicação das Normas pela CVM

A CVM é autorizada conforme a Lei nº 6.385 de 1976 a impor as seguintes penalidades em caso de violação de qualquer disposição de tal lei, sua regulamentação, bem como, quaisquer outras disposições legais, sem prejuízo de eventual responsabilidade civil ou criminal: (i) advertência; (ii) multa[5]; (iii) suspensão do exercício de cargo de administrador ou conselheiro fiscal de companhia aberta, de entidade do sistema de distribuição ou de outras entidades que dependam de autorização ou registro da CVM; (iv) inabilitação temporária, até um período máximo de 20 anos, para o exercício dos cargos referidos no item (iii); (v) suspensão da autorização ou registro para execução das atividades supervisionadas pela CVM; (vi) cassação da autorização para conduzir as atividades supervisionadas pela CVM; (vii)

[5] A multa não excederá o maior das seguintes quantias: (i) R$ 50.000.000,00 (cinquenta milhões de reais); (ii) o dobro do valor da emissão ou da operação irregular; (iii) 3 (três) vezes o montante da vantagem econômica obtida ou da perda evitada em decorrência do ilícito; ou (iv) o dobro do prejuízo causado aos investidores em decorrência do ilícito.

proibição temporária de praticar determinadas atividades ou operação, até um período máximo de 20 anos; (viii) proibição temporária para operar, direta ou indiretamente, em uma ou mais modalidades de operação no mercado de valores mobiliários por um período máximo de 10 anos [6].

7.1.4 Envio de Informações à CVM e Divulgação das Carteiras dos Fundos

Entre outras obrigações, a Gestora deve disponibilizar mensalmente à CVM as informações referentes à composição das carteiras dos Fundos CVM. No caso em que tais Fundos detenham posições ou operações em curso que poderiam ser prejudicadas por sua divulgação, as informações à CVM com relação à composição de sua carteira podem omitir sua identificação e quantidade, registrando somente o valor e sua porcentagem em relação ao total de ativos da carteira. Entretanto, as operações omitidas serão divulgadas dentro de um prazo máximo de 30 (trinta) dias, não prorrogável, para os Fundos CVM classificados como "Renda Fixa", e para todas as outras classes de fundos, 90 (noventa) dias a partir do final do mês, prazo esse passível de prorrogação por igual período, mediante aprovação pela CVM, totalizando o prazo máximo de 180 (cento e oitenta) dias, nos termos da Instrução CVM 555.

Quando da divulgação de dados acerca da composição da carteira dos Fundos CVM, deve ser observado o disposto no art. 56, inciso III, da Instrução CVM 555, e dessa forma garantir o tratamento equitativo aos cotistas.

Os Colaboradores, portanto, somente estão autorizados a divulgar dados da carteira dos Fundos CVM desde que já divulgados ordinariamente pelo administrador fiduciário para a base de dados da CVM, incluindo em reuniões presenciais, documentos individuais para Investidores ou apresentações institucionais. Não se admite divulgação seletiva da carteira (isto é, apenas para alguns Investidores e em periodicidades diferentes).

7.2 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* garantirá, continuamente, que:

[6] As penalidades dispostas nos itens IV a VIII somente serão aplicáveis quando existir um descumprimento de infração grave, conforme definido pelas regras da CVM.

- Os registros na CVM e na ANBIMA sejam atualizados, conforme exigido, bem como que a Gestora esteja cumprindo com regulamentações estrangeiras que sejam aplicáveis às suas atividades;
- O envio de informações à CVM e à ANBIMA seja realizado correta e tempestivamente;
- Os dados das carteiras dos Fundos CVM sejam divulgados de forma equitativa aos Investidores do respectivo Fundo CVM e de acordo com as políticas da Gestora; e
- A M Square mantenha todos os documentos listados acima e exigíveis conforme disposto no Art. 14 da Instrução CVM 558, na regulamentação ou autorregulação aplicável, em sua forma mais atualizada, disponíveis em seu website.

8 Obrigações de envio de informações/documentos – Brasil

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

O(A) Diretor(a) de Risco e *Compliance*, com a assistência dos assessores jurídicos da Gestora, garantirá que todos os documentos e informações exigidos pelas autoridades reguladoras estão sendo enviados tempestivamente.

8.1 Informações Periódicas

Informações	Prazo	Destinatário	Forma de Arquivamento
Enviar à CVM o Anexo 15-II da Instrução CVM 558 devidamente preenchido, contendo informações sobre os Veículos de Investimento sob gestão, profissionais, estrutura administrativa e operacional etc.	Até o dia 31 de março de cada ano, com base nas posições de 31 de dezembro do ano anterior	CVM	Internet (por meio do site da CVM)
O(A) Diretor(a) de Risco e *Compliance* deverá encaminhar ao Comitê de Risco e *Compliance* relatório dos controles internos, regras e procedimentos estabelecidos nesta política (e.g. testes de segurança nos sistemas, medidas para manter as informações confidenciais, programas de treinamento)	Até o último dia útil de abril de cada ano, com base nas informações do ano civil imediatamente anterior	Comitê de Risco e *Compliance*	Físico ou Eletrônico
Confirmar que as informações cadastrais continuam válidas	Até o dia 31 de março de cada ano	CVM	Site da CVM

Informações	Prazo	Destinatário	Forma de Arquivamento
Apresentar Declaração Eletrônica de Conformidade – DEC (pessoas físicas jurídicas e administradores de fundos de investimento)	Até o dia 31 de março de cada ano	CVM	Site da CVM
Informar sobre sua equipe de gestão de investimento, especialmente alterações na equipe	Imediatamente após a ocorrência do evento	ANBIMA	Internet (através do banco de dados de ANBIMA)
Informações	**Prazo**	**Destinatário**	**Forma de Arquivamento**
Confirmar que os profissionais da equipe de gestão são certificados pela ANBIMA e que as informações de valor das cotas dos fundos de investimento foram enviadas.	Até 31 de março, com base nas informações de 31 de dezembro do ano anterior	ANBIMA	Site da ANBIMA
Reportar ao COAF e CVM, se for o caso, a não ocorrência de propostas, transações ou operações passíveis de serem	Até 31 de janeiro de cada ano, com base no ano imediatamente anterior	COAF	SISCOAF

Informações	Prazo	Destinatário	Forma de Arquivamento
comunicadas nos termos da Lei 9.613/98, tendo por base o ano imediatamente anterior			

8.2 Informações Eventuais

Essas informações somente serão arquivadas se determinadas circunstâncias forem verdadeiras.

Informações	Prazo	Destinatário	Forma de Arquivamento
Início ou final dos períodos de distribuição de cotas dos fundos de investimento fechados	Até 10 dias antes do início do período de distribuição e até 10 dias após o final do período de distribuição	CVM	Site da CVM
Voto adotado nas assembleias de acionistas dos Fundos CVM.	Mensalmente	CVM	Site da CVM

Informações	Prazo	Destinatário	Forma de Arquivamento
Em cada momento em que o conjunto de veículos de investimento gerenciado pelo mesmo gestor de investimento ultrapassar, para cima ou para baixo, os patamares de 5%, 10%, 15%, e assim sucessivamente, de qualquer classe de valores mobiliários emitidos por uma companhia listada.	Imediatamente após a ocorrência do evento	Companhia listada que emitiu os valores mobiliários	Carta ou qualquer outro modo definido pela administração do(s) fundo(s) de investimento
Suspeita de lavagem de dinheiro ou atividades de financiamento de terrorismo, conforme definido na Lei 9.613/98.	24 horas após a ocorrência do evento	COAF	SISCOAF
Registrar a versão mais completa e atualizada da Política de Voto junto à ANBIMA.	No momento da adesão e sempre que atualizada	ANBIMA	Via Sistema SSM da ANBIMA
Registrar a versão mais completa e atualizada do Manual de Gerenciamento de Liquidez junto à ANBIMA.	No momento da adesão e no prazo de 15 (quinze) dias sempre que houver atualização	ANBIMA	Via Sistema SSM da ANBIMA

Informações	Prazo	Destinatário	Forma de Arquivamento
Comunicar o administrador fiduciário sobre eventos de iliquidez dos ativos financeiros componentes da carteira dos Veículos de Investimento.	Imediatamente	Administrador	Físico ou eletrônico

8.3 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance*, com a assistência dos assessores jurídicos da Gestora, garantirá que todos os documentos e informações exigidos pelas autoridades reguladoras estão sendo enviados tempestivamente.

ANEXO III

POLÍTICA DE SELEÇÃO E CONTRATAÇÃO DE COLABORADORES

1 Objetivo

O objetivo desta política é estabelecer os procedimentos para a seleção e admissão de novos Colaboradores da M Square, de maneira a buscar a permanente elevação da capacitação técnica de seus profissionais, bem como a observância de padrões de conduta no desempenho de suas respectivas atividades.

Além disso, esta política dispõe sobre os procedimentos necessários a serem adotados para que a M Square atenda às regras do Código ANBIMA de Regulação e Melhores Práticas – Programa de Certificação Continuada.

2 Processo de seleção e admissão de colaboradores

Quando da contratação de novos Colaboradores, a Gestora deverá verificar se os candidatos:

- Possuem reputação ilibada;
- Não tenham sido inabilitados para o exercício de cargo em instituições financeiras e demais entidades autorizadas a funcionar pelo Banco Central do Brasil ou pela CVM, Previc (Superintendência Nacional de Previdência Complementar) ou Susep (Superintendência de Seguros Privados);
- Sua autorização para o exercício da atividade não tenha sido suspensa, cassada ou cancelada; e
- Não tenham sofrido punição definitiva, nos últimos 5 (cinco) anos, em decorrência de sua atuação como administrador ou membro de conselho fiscal de entidade sujeita ao controle e fiscalização dos órgãos reguladores mencionados anteriormente.

Ainda, a Gestora deverá disponibilizar aos Colaboradores admitidos cópia de seu Manual de *Compliance*, Código de Ética, e demais políticas aplicáveis, sendo certo que estes deverão ler, compreender e cumprir integralmente os documentos, aderindo a estes por escrito, por meio da assinatura do Termo de Adesão.

Além disso, faz parte do programa de *Compliance* da Gestora a realização de treinamentos iniciais para seus Colaboradores, ocasião em que serão abordados temas objeto deste Manual, tais como:

princípios éticos, regras de conduta, investimentos pessoais, regras de confidencialidade das informações, combate à lavagem de dinheiro e corrupção, dentre outras políticas relevantes.

3 Concessão de acessos aos sistemas da gestora

Quando do ingresso de um novo Colaborador ou da sua promoção/mudança de área interna, a área de *Compliance* deverá analisar as credenciais de acesso às instalações físicas do escritório e o acesso aos recursos computacionais utilizados pela Gestora, tais como sistemas eletrônicos e diretórios internos, os quais deverão ser concedidos ao respectivo Colaborador, em razão das atividades que este exercerá.

4 Desligamento de colaboradores

Nos casos de desligamento de Colaboradores, a área de *Compliance* deverá tomar providências com relação ao encerramento dos acessos destes, seja ao escritório ou aos dispositivos e sistemas eletrônicos de propriedade da Gestora.

Cabe, ainda, a área de *Compliance*, em conjunto com a área de TI, assegurar a "limpeza" de dados de máquinas (formatação do disco rígido) e instalações relativas ao Colaborador desligado.

Adicionalmente, se for o caso, para aqueles Colaboradores que atuem em posição sujeita à certificação ANBIMA, deverá ser observado o disposto na Política de Certificação Continuada de Colaboradores, conforme Anexo VIII do presente Manual.

5 Análise e acompanhamento da regulamentação e autorregulação

É de responsabilidade da área de *Compliance* o acompanhamento da regulamentação e autorregulação que disponha sobre os requisitos para o exercício, pelos Colaboradores, das atividades objeto da Gestora.

Este procedimento consiste, em especial, na verificação das atividades desenvolvidas pelos Colaboradores que estejam sujeitas à obtenção de certificação ANBIMA com base no Código ANBIMA de Regulação e Melhores Práticas - Programa de Certificação Continuada. Assim, a Gestora deverá adotar critérios que determinem as atividades elegíveis às certificações, e selecionar para desempenhá-las, Colaboradores capacitados, devendo ainda realizar testes de aderência periódicos em relação ao cumprimento desta Política.

6 Revisão de *Compliance* e procedimentos operacionais

De acordo com a Instrução CVM 558 e autorregulação da ANBIMA aplicável, a Gestora deve assegurar que seus profissionais não deixem de gozar da reputação ilibada. Assim, os Colaboradores deverão prontamente comunicar o(a) Diretor(a) de Risco e *Compliance*, através do e-mail *Compliance*@msquare.com.br, acerca de processos judiciais ou administrativos instaurados contra si, e questões midiáticas negativas o envolvendo (ex. envolvimento em atos de corrupção, esquemas de lavagem de dinheiro, etc.).

Ademais, a área de *Compliance* deverá realizar pesquisas na internet de seus Colaboradores, e, com relação aos sócios controladores diretos e indiretos e diretores da Gestora, a Gestora usa uma empresa especializada em *background checks* para as pesquisas anuais dos socios controladores e novos Colaboradores.

Caso sejam encontrados apontamentos em nome dos sócios controladores diretos e indiretos e diretores da M Square, o *Compliance* deverá avaliar a necessidade de: (i) *disclosure* no Formulário de Referência e/ou formulários de *Due Diligence* padrão ANBIMA ou respondido a investidores; (ii) *disclosure* a determinados investidores em razão de *side letters* firmadas; e (iii) necessidade de afastamento do respectivo sócio ou diretor, em razão da necessidade de manutenção permanente de reputação ilibada, conforme acima mencionado.

ANEXO IV

POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E PREVENÇÃO DE CONFLITOS DE INTERESSES

1 Objetivo

O objetivo desta política é implementar mecanismos internos que assegurem a correta utilização de informações, dados e estratégias de operações da M Square, bem como de seus Veículos de Investimentos, clientes ou investidores.

Considerando (i) que a M Square possui participação societária em sociedade que presta serviços de consultoria a fundos de investimento, sociedades ou entidades constituídos no exterior, relacionadas a investimentos ou oportunidades de negócios no exterior ("Base Partners"); e (ii) eventual presença física de profissionais de outras sociedades no endereço comercial da M Square, é necessário estabelecer as diretrizes a serem observadas pelos Colaboradores destas diferentes áreas, garantindo, assim, o devido nível de acesso de cada um às informações confidenciais de sua respectiva área, em especial, da área de gestão de recursos de terceiros.

Desta forma, as diretrizes elencadas nesta política possuem como objetivo:

- Garantir a segregação entre a área responsável pela gestão de recursos de terceiros e outras atividades desenvolvidas no endereço comercial da Gestora;
- Garantir a segregação entre a área responsável pela gestão de recursos de terceiros da M Square e quaisquer outros Representantes de terceiros que, eventualmente, ocupem espaço físico nas instalações da Gestora;
- Assegurar o bom uso de instalações, equipamentos e informações comuns a mais de uma área; e
- Preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

2 Áreas segregadas

Tendo em vista a natureza das atividades desempenhadas pela M Square, é necessária a implementação de estruturas segregadas entre a área responsável pela gestão de recursos de terceiros e as demais atividades acima mencionadas, as quais possuem controle informacional e lógico (sistemas, diretórios internos e rede corporativa) distintos.

A segregação existente entre as sociedades não afasta a possibilidade de sócios e Colaboradores das sociedades interagirem para a tomada de decisões, tendo em vista o vínculo societário e estratégico existente entre as sociedades, bem como a complementariedade de seus negócios, conforme devidamente divulgado no Formulário de Referência da M Square.

2.0 Procedimentos de Segregação

Em consonância com o disposto na citada Política de Seleção e Contratação de Colaboradores, a área de *Compliance*, em conjunto com a área Administrativa, são responsáveis por conceder os acessos aos sistemas, diretórios internos e rede corporativa aos Colaboradores, de acordo com as atividades por estes exercida.

Nesse sentido, a M Square implementou mecanismos de segregação informacional que garantem que os Colaboradores das demais áreas e sociedades citadas acima não possuem acesso a informações e documentos confidenciais da área de gestão de recursos de terceiros.

2.1 Utilização de Áreas Comuns

Os Colaboradores não devem compartilhar informações confidenciais em áreas comuns abertas, tais como copa, corredor, elevadores, etc.

As reuniões devem ocorrer em salas fechadas, devendo os Colaboradores dispensar especial atenção para não deixar papéis, rascunhos, materiais e apresentações de cunho confidencial em salas de reunião e impressoras compartilhadas.

Ao terminar uma reunião, o Colaborador deve verificar que não há material esquecido, tampouco sistemas abertos, ou qualquer outro dado que possa ser confidencial.

2.2 Segregação das atividades da Diretora responsável pela Administração de Carteiras de Valores Mobiliários

No que tange à segregação da atividade do(a) Diretor(a) de Investimentos, é importante ressaltar que sua independência é requisito essencial regulamentar e está intrinsecamente ligada à cultura da M Square.

Nesse sentido, tal Diretora não pode ser responsável por nenhuma outra atividade no mercado de capitais, na instituição ou fora dela, salvo a exceção permitida pela CVM, como é o caso de atuação desta Diretora como conselheira de companhia aberta ou não, nos termos do Ofício-Circular

CVM/SIN/N. 5/2014. Ainda assim, esta hipótese deverá requerer aprovação prévia do Comitê de Risco e *Compliance*, para análise e implementação dos devidos procedimentos.

2.4 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* é responsável por fiscalizar a efetiva segregação de atividades aqui estabelecida, monitorando o acesso a documentos, informações e ambientes exclusivos de cada área, bem como o bom uso dos espaços comuns a todas as áreas.

Caso seja detectada insuficiência nos procedimentos internos de manutenção da segregação ou o descumprimento dos procedimentos aqui estabelecidos, os Colaboradores da área de gestão deverão empreender seus melhores esforços para evitar qualquer prejuízo à M Square, seus Veículos de Investimento, clientes ou investidores, bem como para reparar qualquer falha, se existente.

Caso ocorra qualquer falha nos procedimentos aqui definidos, o(a) Diretor(a) de Risco e *Compliance* deverá manter arquivo contendo o registro de todas as ocorrências relacionadas a necessária segregação de atividades entre as áreas aqui estabelecidas, elencando, no mínimo:

- Descrição da falha identificada;
- Forma de detecção da falha;
- Prejuízos verificados, se aplicável;
- Plano de ação e saneamento; e
- Necessidade de aplicação de medidas coercitivas ou preventivas.

3.0 Conflitos de interesses e regras de alocação em sociedades ligadas

Em regra, a M Square não investe em ativos emitidos ou assessorados por sociedades ligadas a M Square ou seus sócios, tal como a Base Partners ou suas subsidiárias, por conta e ordem dos Veículos de Investimento.

Entretanto, potencialmente, tal investimento poderá ser considerado como sendo a melhor decisão de investimentos, no melhor interesse dos clientes e investidores, de acordo com: (i) as políticas de investimentos de cada Veículo de Investimento; (ii) o cenário do momento em questão; e (iii) interesses específicos de investidores de fundos internacionais, Fundos CVM Exclusivos, Restritos ou Reservados.

Nesta hipótese, para evitar qualquer conflito potencial na alocação de operações, deverão ser adotadas as seguintes regras:

- É vedado aos Fundos CVM aplicar nos ativos de sociedades ligadas. Qualquer exceção deverá ser aprovada pelo Comitê de Investimentos, em conjunto com o Comitê de Risco e *Compliance*;
- Investidores que tenham potencial interesse em investir nos ativos de emissão ou assessoramento da Base Partners ou suas subsidiárias, serão incentivados a avaliar a possibilidade de implementar tais investimentos através de outros veículos que não geridos pela M Square.;
- No caso de Fundos *Offshore*, Fundos CVM Exclusivos, Restritos ou Reservados, a M Square deverá sempre obter o aval do investidor ou seu representante, anteriormente a qualquer investimento junto à Base Partners;
- É permitida a gestão de relacionamento de clientes comuns ou compartilhados com a outra sociedade, quando não houver violação de dever confidencialidade. Na comunicação entre os profissionais da M Square e a Base Partners não devem ser trocadas informações de cunho confidencial dos Veículos de Investimento, conforme exemplificado abaixo; e
- Devem ser integralmente respeitadas as regras de segregação de atividades dispostas nesta Política.

São exemplos de informações que não devem ser trocadas entre a M Square e a Base Partners, nos termos da Política de Confidencialidade da Gestora: informações sobre movimentações dos Veículos de Investimento por seus investidores, informações sobre movimentações que possam impactar na liquidez e *valuation* dos Veículos de Investimento, informações institucionais e estratégicas sobre a Gestora.

4.0 Procedimentos Operacionais e revisão De *Compliance*

O(A) Diretor(a) de Risco e *Compliance* garantirá, continuamente, que o disposto neste item seja cumprido, devendo conduzir revisão anual sobre o permanente atendimento aos itens acima dispostos.

ANEXO V

POLÍTICA DE DECISÃO DE INVESTIMENTOS E DE SELEÇÃO E ALOCAÇÃO DE ATIVOS E INVESTIMENTOS NO EXTERIOR

1 Objetivo

Esta Política tem por objetivo traçar as diretrizes a serem observadas pelos Colaboradores, notadamente os integrantes da equipe de Gestão, no processo de decisão de investimentos e alocação de ativos por conta e ordem dos fundos de investimento domiciliados no Brasil, ou investidos pelos fundos de investimentos domiciliados no Brasil por ela geridos (conjuntamente referidos como "Veículos de Investimento").

2 Diretora de gestão e estrutura da área

A Diretora responsável pela atividade de administração de carteiras de valores mobiliários da M Square é a Sra. Luciana Barreto Gattass ("Diretora de Investimentos"), a quem incumbe a responsabilidade final pelas decisões de investimento em nome dos Veículos de Investimento. Em suas atribuições, é assessorada diretamente pelo Comitê de Investimentos.

3 Comitê de investimentos

A M Square possui um Comitê de Investimentos, composto pelos sócios e analistas da área de investimentos e coordenado pela Diretora de Investimentos, que tem por finalidade principal discutir as estratégias de decisão de investimento e alocação de ativos sob gestão da M Square (incluindo os Veículos de Investimento).

A partir da discussão e avaliação constante dos cenários, premissas e dados fornecidos pelos membros da equipe de Gestão, o Comitê auxilia a Diretora de Investimentos sobre a melhor composição das carteiras dos Veículos de Investimento.

O Comitê de Investimentos se reúne ao menos mensalmente, e sempre que necessário, mediante convocação de qualquer de seus membros, para discutir quaisquer assuntos que se mostrem relevantes para o processo de decisão de investimentos e alocação de ativos. A convocação se dará por e-mail aos demais membros do Comitê.

De forma não exaustiva, faz parte da competência do Comitê de Investimentos:

- Orientar a equipe de Gestão na busca de oportunidades compatíveis com os Veículos de Investimento;
- Avaliar as opções de investimento, suas relações risco/retorno, e sua aderência aos regulamentos e políticas de investimentos de cada Veículo de Investimento;
- Solicitar informações adicionais na busca de mitigar riscos percebidos na análise de cada investimento; e
- Auxiliar o(a) Diretor(a) de Investimentos na escolha e aprovação de investimentos e desinvestimentos dos Veículos de Investimento.

O Comitê de Investimentos arquivará em sistema eletrônico ou arquivo físico todos os materiais de trabalho que servem de apoio para fundamentar as suas discussões e decisões aprovadas nas respectivas reuniões do Comitê pelo prazo mínimo de 5 (cinco) anos.

4 Processo de gestão de portfólio: análise, seleção e monitoramento de gestores de recursos de terceiros

O processo de gestão de portfólio desenvolvido pela M Square é executado de forma que a Gestora possa cumprir suas obrigações de forma sistemática e consistente, sempre protegendo os interesses de seus clientes.

A abordagem praticada pela M Square é prioritariamente *bottom-up*, com ênfase na análise específica de risco-retorno de cada um dos ativos.

A M Square adota como principal estratégia para os Veículos de Investimento a seleção diligente e minuciosa de gestores de recursos localizados principalmente nos Estados Unidos da América e Europa com comprovado *track record* e expertise em suas respectivas áreas de atuação. Os Veículos de Investimentos têm seus ativos majoritariamente alocados em cotas de fundos de investimentos sediados no exterior.

Para seleção e análise das oportunidades de investimento, os membros da equipe de Gestão se baseiam na sua expertise, sólido conhecimento internacional e análise contínua dos ativos e estratégias pertencentes às carteiras dos Veículos de Investimento.

Em especial, são constantemente realizadas pesquisas e diligências acerca dos gestores de recursos de terceiros selecionados, bem como daqueles ativos que se pretenda adquirir, ou novos gestores que se pretenda investir, considerando: (i) as diversas classes de ativos disponíveis; (ii) os cenários

econômico e político, nacional e internacional; (iii) as políticas de investimento de cada Veículo de Investimento; e, (iv) suas eventuais restrições especificadas no contrato de gestão e/ou no seu regulamento / *PPM- Private Placement Memorandum*.

Mais especificamente, a estratégia de investimentos da M Square tem foco no longo prazo e adota uma abordagem de investimento baseada em análise fundamentalista. Procura investir em fundos geridos por terceiros que adotem estratégias simples e resilientes, cujos gestores tenham talento comprovadamente superior se comparado a seus pares globais, e cujo alinhamento de interesses seja amplo com os seus clientes.

O foco da análise são gestores cujo sucesso dependa mais de análises microeconômicas de ativos específicos dos que da situação macro. Características comuns aos Fundos Investidos nos quais a M Square busca alocar recursos dos Veículos de Investimentos são:

- Primordialmente fundos de investimento de gestores independentes, cujo foco seja gerir especificamente a carteira na qual a M Square investe;
- Fundos de investimento que empreguem estratégias simples. Consideramos estratégias simples aquelas que possam ser facilmente descritas (e compreendidas). No caso dos Veículos de Investimento, o foco é em renda variável *long only*, renda variável *long biased*;
- Fundos de investimento que não usem alavancagem financeira;
- Gestores alinhados (com muito de seu capital próprio investido no mesmo fundo que a M Square) e com histórico comprovado dentre os melhores entre seus pares globais;
- Gestores que disponibilizam à M Square acesso aberto e frequente;
- Fundos de investimento com portfolios prudentemente diversificados, e com controle de risco apropriado para a sua estratégia; e
- Fundos de investimento que ofereçam liquidez apropriada para a estratégia em questão.

Em outras palavras, os Veículos de Investimentos da M Square tendem a ser compostos por fundos de investimento que embora possam ser voláteis no curto prazo, tenham uma baixa chance de gerar perdas permanentes de capital devido à combinação de suas estratégias e construção de portfólios.

As estratégias adotadas pela M Square no processo de gestão de portfólio poderão ser alteradas levando em conta mudanças microeconômicas ou outros fatores a critério do Comitê de Investimentos, e desde que dentro dos parâmetros de risco e *Compliance* previamente estabelecidos.

4.1. Fundos Exclusivos ou Reservados

Em relação aos Veículos de Investimento que sejam Exclusivos, Restritos ou Reservados, nos termos da regulamentação brasileira, ou ainda eventuais carteiras administradas, constituídos para investidores profissionais, nos termos da regulamentação da CVM, a M Square poderá eventualmente consultar investidores anteriormente à realização de operações em nome de tais Veículos de Investimento, mas sempre selecionando os ativos de forma discricionária, e cabendo à M Square a decisão de investimento final. Não obstante, ainda que com ingerência do investidor, notadamente o representante do quotista de Fundo Exclusivo, Restrito ou Reservado, a seleção e decisão dos investimentos deve necessariamente passar pelo processo padrão descrito nesta Política, inclusive com o crivo do Comitê de Investimentos.

Em nenhuma hipótese, a influência do investidor na gestão dos Veículos de Investimento pode ser utilizada como mitigador de responsabilidade acerca do dever de diligência da Gestora na análise, seleção e monitoramento de investimentos sob sua gestão.

4.2. Negócios em Mercados e Emissores Estrangeiros

A M Square tem como política investir em cotas de fundos estrangeiros como parte de suas estratégias de investimento, em linha com as políticas de investimento constantes dos regulamentos dos Veículos de Investimento.

A Gestora investirá indiretamente em gestores de recursos de terceiros estrangeiros, devidamente registrados por autoridade estrangeira competente, através do investimento nas cotas de fundos estrangeiros geridos pela própria gestora.

Quando a M Square investir em contas de fundos de investimento estrangeiros em nome dos Veículos de Investimento, ainda que geridos pela própria Gestora, deverá considerar as exigências da Instrução CVM n. 555/14, em especial o previsto nos seus arts. 98 a 101.

A M Square deverá ser diligente com relação às restrições de investimento dos regulamentos ou contratos dos Veículos de Investimento ao determinar elegibilidade de determinado investimento em emissores estrangeiros, especialmente com relação as seguintes questões:

- fundo ou veículo estrangeiro seja constituído, regulado e supervisionado por autoridade local reconhecida;
- possua o valor da cota calculado a cada resgate ou investimento e, no mínimo, a cada 30 (trinta) dias;

- possua administrador, gestor, custodiante ou prestadores de serviços que desempenhem funções equivalentes, capacitados, experientes, de boa reputação e devidamente autorizados a exercer suas funções pela CVM ou por autoridade local reconhecida;
- possua custodiante supervisionado por autoridade local reconhecida;
- tenha suas demonstrações financeiras auditadas por empresa de auditoria independente; e
- possua política de controle de riscos e limites de alavancagem compatíveis com a política do fundo investidor.

Todo e qualquer novo investimento no exterior, uma vez aprovado pelo Comitê de Investimentos, deverá passar previamente pela análise do(a) Diretor(a) de Risco e *Compliance*, para verificações acima sobre a jurisdição, gestor ou ativo, conforme o caso, bem como sua averiguação junto a área de *backoffice* acerca dos detalhes para correta liquidação da operação no novo mercado, ou com relação a um novo gestor/ativo, conforme o caso.

4.2.1 Procedimentos Operacionais e Revisão de *Compliance*

O(A) Diretor(a) de Risco e *Compliance* garantirá, continuamente, que o disposto neste item seja cumprido, devendo conduzir revisão anual sobre o permanente atendimento aos itens acima dispostos.

5 Contratos de Gestão

O(A) Diretor(a) de Risco e *Compliance* e o(a) Diretor(a) de Investimentos deverão revisar cada Contrato de Gestão, ou instrumento equivalente, a ser celebrado com os investidores em potencial, de modo a garantir que todas as disposições exigidas estejam presentes.

6 Gestão de caixa dos fundos

Como política de gestão de caixa dos Veículos de Investimento, todo o saldo de caixa é investido em (i) títulos públicos, quando os ativos estão em moeda local ou (ii) mantidos em caixa ou investidos em títulos do governo norte-americano (T-Bills) de forma direta ou indireta (via fundos de Money Market) quando os ativos estão em dólares norte-americanos. Os Veículos de Investimento geridos pela M Square não incorrem diretamente, portanto, em risco de crédito privado.

7 Crédito Privado

Atualmente, a M Square adquire essencialmente cotas de fundos de investimento, que embora possam ser consideradas tecnicamente como “crédito privado” em oposição às demais categorias disponíveis, seu modo de seleção e monitoramento difere dos títulos de dívida privada regulamentados como tal.

Caso a M Square venha a selecionar e adquirir diretamente ativos de Crédito Privado, ou seja, títulos representativos da dívida de empresas e instituições privadas, a área de análise responsável seguirá procedimentos próprios de diligência, pesquisa e monitoramentos em relação aos emissores do crédito, mensurando os riscos associados aos ativos investidos e, cumulativamente, observando as diretrizes publicadas pela ANBIMA e CVM sobre o tema, em especial o Ofício-Circular CVM/SIN/N. 6/2014. Assim, caso a M Square venha a atuar diretamente neste segmento, deverá possuir uma Política própria que disciplinará sua atuação se e quando exercer a escolha discricionária de ativos de crédito privado para os Fundos CVM.

ANEXO VI

POLÍTICA DE RATEIO E DIVISÃO DE ORDENS

1 Introdução

Os gestores de recursos de terceiros possuem um dever afirmativo de atuar de boa-fé para o benefício de seus clientes e, no âmbito do seu dever fiduciário. Nesse sentido, os gestores de recursos de terceiros devem garantir que, ao alocar e agregar as transações de valores mobiliários, os clientes sejam tratados de uma forma absolutamente justa e equitativa.

2 Alocação de ordens

Atualmente, a M Square possui como procedimento principal que as ordens de compra e venda em nome dos Veículos de Investimento sejam expedidas com a identificação do beneficiário final, tendo em vista que a Gestora atualmente investe, essencialmente em cotas de fundos de investimentos geridos e administrados por terceiros, sobretudo no exterior.

Nos casos em que a Gestora utilizar o procedimento de rateio de ordens agrupadas, serão considerados para rateio de ordens, o perfil de risco, a alocação e peso por estratégia de cada cliente, além do mínimo exigido pelos fundos de investimentos.

As aplicações para sócios e funcionários da M Square podem ter um mínimo diferente do mínimo exigido dos clientes. Os investimentos feitos pelos sócios têm como objetivo o alinhamento de interesses dos sócios com os clientes nas recomendações de investimentos.

Cabe a(o) Diretor(a) de Risco e *Compliance* revisar esta Política para prever critério equitativos e verificáveis de rateio, anteriormente à realização de tal procedimento.

2.1 Potenciais Conflitos de Interesses entre a Gestora e sociedades coligadas, controladas ou do mesmo Conglomerado / Grupo Econômico

Tendo em vista a natureza de suas atividades, conforme acima mencionado, a M Square não atua na contraparte da própria Gestora, seus Colaboradores, ou de veículos e sociedades coligadas, controladas ou controladoras, nem tampouco faz parte de Conglomerado / Grupo Econômico; portanto, não são vislumbrados potenciais conflitos de interesses com intermediários financeiros ou contrapartes relacionadas em operações dos fundos de investimento.

ANEXO VII

PLANO DE CONTINGÊNCIA E RECUPERAÇÃO DE DESASTRE

1 Introdução

1.1 Objetivo

A M Square Investimentos Ltda. ("**Empresa**" ou "**M Square**") elaborou este plano de contingência e recuperação de desastre (o "**Plano de Contingência**") com o objetivo de estabelecer os procedimentos adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais da empresa como um todo ("**Eventos de Contingência ou Desastre**") com vistas a assegurar à M Square e seus colaboradores a plena continuidade operacional das atividades da empresa, a todo tempo e sob qualquer circunstância.

São exemplos de Eventos de Contingência ou Desastre: suspensão total ou interrupção temporária na prestação de serviços por provedores de energia, acesso à internet, serviços de telefonia, etc., catástrofes naturais que impeçam o acesso ao prédio, interdição do prédio onde funciona a sede da M Square por qualquer motivo, inclusive em cenários de greves, pane nos sistemas e softwares utilizados pelos Colaboradores da Empresa, perda de arquivos por qualquer motivo, dentre outros.

Dentre as funcionalidades críticas à M Square a que este Plano de Contingência se propõe a cobrir incluem-se (i) a contínua execução de trades (com a respectiva manutenção das regras de *Compliance* aplicáveis), (ii) o desempenho das rotinas operacionais, (iii) a possibilidade de recebimento e troca regular de e-mails (sejam internos ou com contrapartes externas) e atendimento telefônico via PABX além de (iv) acesso/uso ininterrupto aos sistemas, funcionalidades e arquivos utilizados pela Empresa, conforme descritos no item 1.2 abaixo ("**Sistemas Cobertos**"), mesmo em caso de total impossibilidade de acesso ao escritório físico da Empresa.

1.2 Funcionalidades e Sistemas Cobertos

São funcionalidades e sistemas cobertos para fins deste Plano de Contingência:

- E-mails & Intranet;
- Sharepoint;
- Sistema de Passivo e Carteiras Offshore: PackHedge

- Sistema de Passivo e Carteiras Onshore: Phibra
- *Bloomberg*; e
- Fileserver.

2 Medidas Preventivas

A M Square adota as seguintes medidas preventivas visando a mitigação de eventuais riscos de ocorrências de Eventos de Contingência ou Desastre:

A. **Rota de fuga, sinalização de emergência e simulações de incêndio:** a sinalização das rotas de fuga e colocação da sinalização de emergência é feita em locais estratégicos do escritório da Empresa e facilmente identificáveis. Os colaboradores são ainda, instruídos à se portarem com um padrão de conduta adequado em caso de incidentes com fogo. Neste caso, os colaboradores são obrigados a participar das simulações periódicas de incêndio realizadas pelo condomínio de modo a se familiarizarem com os procedimentos mínimos exigidos para o caso de uma ocorrência que demande a evacuação do prédio.

B. **Identificação de visitantes / Circulação de terceiros:** com vistas a assegurar um nível de segurança mínimo nas suas premissas, os visitantes serão permitidos a subir ao escritório da M Square mediante prévia aprovação de um dos colaboradores. Neste mesmo sentido, os visitantes e prestadores de serviços são instruídos a observar o procedimento padrão para circulação dentro do escritório, não sendo permitida sua entrada no salão principal exceto se acompanhado de um colaborador. Ademais, a entrada de colaboradores no escritório e salão principal é controlada por sistema de biometria.

C. **Monitoramento do Ambiente Corporativo:** o monitoramento do ambiente corporativo se dá através da instalação de câmeras em locais estratégicos do escritório, permitindo a identificação de quem acessa o escritório, com a respectiva retenção dasgravações.

D. **Avaliação Periódica dos Circuitos Elétricos:** a Empresa, através de prestadores de serviços terceirizados, realiza a reavaliação dos circuitos elétricos de seu escritório com vistas a mitigar possíveis riscos.

E. **e Instalações Hidráulicas:** o condomínio, através de prestadores de serviços terceirizados, realiza periodicamente a manutenção do sistema hidráulico dos andares com vistas a mitigar riscos de rompimento e/ou defeito das instalações hidráulicas (registros, válvulas e pontos deinfiltração).

F. **Telefones de Colaboradores:** a Empresa disponibiliza aos seus colaboradores - em sua intranet - o acesso à lista de telefones celulares pessoais de cada um dos demais colaboradores, inclusive para os casos de emergência, facilitando assim a comunicação em cenários de estresse ou emergenciais.

3 Infraestrutura Tecnológica

A M Square é detentora de uma infraestrutura tecnológica robusta. A Empresa opera com 1 *datacenter* próprio onde ficam localizados seus servidores físicos e virtuais e 1 *datacenter* virtual de *Disaster Recovery,* hospedado na Microsoft. Todos os sistemas de produção e arquivos rodam nos servidores e todos eles têm redundância interna completa (discos e fontes).

Sistemas: Os servidores responsáveis pelos sistemas de produção (Phibra) e bancos de dados da Empresa estão localizados em *datacenter* próprio e replicados para o datacenter virtual (Microsoft).

Servidores Dell operando em modo Virtual através de Hyper-V, de tal maneira que nenhuma falha única cause indisponibilidade sistêmica (*No Single Point of Failure*). O uptime médio está acima de 99.9% ao longo dos últimos 4 anos. Além disso, diariamente é feito um back-up dos arquivos em nuvem (Microsoft Azure) e criptografado.

Arquivos: Os servidores responsáveis pelo sistema de arquivos (*File Server*) da M Square estão localizados em *datacenter* próprio localizado no escritório da M Square – em um ambiente com servidores, *storage* e rede totalmente redundantes (CPD) – e todos os dados desse sistema de arquivos são sincronizados em tempo real, com o ambiente de *Disaster Recovery*. Além disso, diariamente é feito um back-up dos arquivos em nuvem (Microsoft Azure), criptografados e com política de retenção de 10 anos.

E-mail: O sistema de e-mail está localizado fora do escritório (*Microsoft Office 365*), com retenção/armazenamento automático de todos os e-mails por 7 anos. Sendo assim, em caso de um Evento de Contingência ou Desastre, todo o histórico de e-mails estará disponível via *webmail* e o fluxo de entrada e saída de e-mails não será afetado.

Em caso de indisponibilidade da Microsoft, a M Square conta com o serviço de contingência da PROOFPOINT onde os usuários possuem acesso a um mailbox de emergência para acesso durante a indisponibilidade do serviço principal.

Acesso à rede: Todas as permissões de rede/login/senha são sincronizadas online com o ambiente de *Disaster Recovery,* tendo em vista a existência de um *domain controller* da rede. Ou seja, uma

alteração de senha no ambiente de produção é replicada no ambiente de *Disaster Recovery* em questão de segundos, viabilizando desta forma, o acesso remoto à rede com o mesmo login e senha de acesso utilizados no escritório físico.

PABX: Nossa telefonia (PABX e troncos) está na nuvem, em modo de alta disponibilidade. Temos contingência local.

Adicionalmente, ressaltamos que todas as ligações são gravadas e as mesmas ficam disponíveis por 5 anos.

Escritório: O escritório da M Square possui redundância no acesso à internet (4 links), backup de eletricidade (1 nobreak com pelo menos 1 hora de autonomia e 4 geradores no prédio, que entram em serviço em média 19 segundos após uma falta de luz) e 2 fornecedores de telefonia, pois caso um deles falhe, o outro será ativado, permitindo a continuidade dos negócios sem interrupções. Este Plano de Contingência foi estruturado de forma a garantir a manutenção do maior tempo de atividade possível ao nosso escritório.

Provedores de Serviço de TI: A M Square conta um fornecedor externo (Atual - IT) que fica disponível 24/7. Este fornecedor consegue trabalhar remotamente sobre a quase totalidade dos problemas e, caso necessário, está comprometido em mandar um técnico ao escritório em menos de uma hora para suporte.

Disaster Recovery: A estrutura externa de *Disaster Recovery* (ver abaixo "Estrutura e Plano de *Disaster Recovery*") é sincronizada automaticamente e pode ser acessada em Eventos de Contingência ou Desastre, observados os critérios e procedimentos abaixo definidos.

Sumário da Infraestrutura:

Sistemas e Bancos de dados	Localizados em *datacenter* próprio e sincronizados diariamente com um *datacenter* externo de *Disaster Recovery*, além de *backup* em nuvem. Banco de Dados sincronizados em D-1
Arquivos (FileServer)	Localizados em *datacenter* próprio e sincronizados em tempo real com um *datacenter* externo de *Disaster Recovery*, além de *backup* em nuvem.

Arquivos (Sharepoint)	Fluem através de uma solução em nuvem da Microsoft (Office365). Para menor dependência física, a empresa já opera com arquivos chaves em nuvem através do Sharepoint Online. O Sharepoint conta com backup automático e versionamento dos arquivos.
E-mails	Armazenados e fluem através de uma solução em nuvem da Microsoft (Office365), com retenção dos últimos 7 anos. Mailbox de Emergencia provido pelo PROOFPOINT
PABX/ Telefonia	Produção Nuvem e contingência no local.

4 Estrutura para Plano de *Disaster Recovery*

A M Square possui uma estratégia para cenários de desastre composta por (i) *back-ups* de seus sistemas e (ii) estrutura de acesso remoto, com sincronismo diário e completamente disponíveis para uso tanto em caso de um desastre físico envolvendo seu escritório quanto em caso de contingência envolvendo o ambiente de *Disaster Recovery*.

(i) Back-up de Sistemas: com relação aos sistemas, todos os sistemas de produção da Empresa estão localizados em um *datacenter* próprio, com sincronismo diário para um *datacenter* externo hospedado na Microsoft. Além disso, é feito diariamente backup em nuvem e criptografado, para garantir a capacidade de restaurar o ambiente caso algum evento afete o escritório.

(ii) Acesso remoto: A Empresa disponibiliza aos seus colaboradores notebooks corporativos para acesso aos arquivos e sistemas.
A empresa conta com um contrato com a Microsoft para suprir *back-up* de Sistemas, bancos de Dados, *File Server* para manter cenários de contingência.

5 Procedimentos

5.1 Procedimentos durante um Evento de Contingência ou Desastre

- <u>Falha de Sistemas:</u>

No caso de um Evento de Contingência ou Desastre que implique na descontinuidade na prestação de serviço atrelados aos sistemas operacionais considerados críticos – Sistemas Cobertos, e/ou em seus servidores e rede, a detentora dos acessos e controles atuará para reestabelecer o acesso aos referidos sistemas de forma emergencial, além de ativar imediatamente e disponibilizar na rede em modo redundante. Caso tal falha seja decorrente de um Evento de Contingência ou Desastre na qual fique inviabilizado o acesso ao escritório físico da M Square, os colaboradores devem se orientar para que o acesso seja feito remotamente e conforme guia de acesso remoto disponível na Intranet da Empresa.

- Falha de Infraestrutura:

(a) **Energia Elétrica**: caso haja falha no fornecimento de energia, a M Square conta com os seguintes recursos: (i) 1 sistema de alimentação secundária de energia elétrica (nobreak) com 2 horas de autonomia de bateria; e (ii) 4 geradores no prédio inicializados automaticamente que levam em média 19 segundos para ativação após a ocorrência de queda de energia e possuem autonomia de mais 36 horas até que seja necessário seu reabastecimento.

✓ Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, o(a) responsável pelo departamento de T.I orientará para que todos se desloquem até suas casas com seus respectivos Laptops, e deem continuidade operacional aos trabalhos via acesso remoto ao site de contingencia DR..

(b) **Comunicações:** a M Square conta com 4 links de acesso à internet (redundância) para a eventualidade de uma falha na prestação do serviço do provedor de internet e/ou no link de dados.

Da mesma forma, a Empresa possui *back-up* de telefonia.

(c) **Desastres (Incêndio, inundação, assalto, etc):** Eventos de Contingência ou Desastre que impliquem na evacuação e/ou inacessibilidade do escritório físico onde está localizada a sede social da Empresa, impossibilitando o acesso aos sistemas de operação da empresa.

✓ Principais Ações e Responsáveis: Além dos procedimentos padrão de evacuação do edifício e atuação ativa dos brigadistas para salvaguardar a vida dos colaboradores da M Square, ficará a cargo do(a) responsável pela área de TI e em sua ausência, do(a) Diretor(a) de Gestão de Risco da M Square, atuar para viabilizar a ativação do site de contingência, permitindo aos colaboradores, acesso seguro e integral à rede, aos Sistemas Cobertos, aos seus e-mails e

demais recursos mínimos necessários para restabelecimento operacional, sem maiores rupturas.

Para tanto, a orientação aos colaboradores é de procederem às suas residências ou a um local seguro em que possam, através de seus respectivos laptops, acessar o ambiente de contingência através de VPN.

- ✓ Tempo de Ação: Imediato - quanto antes for a atuação da Empresa e de seus colaboradores, menor será o prejuízo. O(A) responsável pela infraestrutura da M Square ficará a inteira disposição dos *Key-Users* para viabilizar os acessos aos Sistemas Cobertos em Eventos de Contingência ou Desastre.

5.2 Acesso ao Ambiente DR

Os procedimentos para acesso a VPN de contingência encontram-se detalhados abaixo:

Neste cenário, os colaboradores permanecem com acesso full aos e-mails (incluindo nos aparelhos celulares). Os sistemas de arquivos estão com a última versão de contato com o site, já que a replicação é em tempo real. Os bancos de dados e sistemas serão restaurados para D-1 na ocasião do evento, sendo necessário refazer as rotinas do dia do desastre.

A Empresa disponibiliza o acesso ao ambiente DR para dois grupos segregados de Colaboradores, quais sejam:

(1) Key Users – áreas consideradas críticas para fins de continuidade do negócio em um Evento de Contingência ou Desastre, são elas: *Trading, Back-office, Compliance* e Relações com Investidores.

(II) Demais Colaboradores

A prioridade de atendimento é para os *Key Users*, seguida de restauração do ambiente de produção e posteriormente, atendimento e acesso aos demais usuários. Em caso de problemas no acesso durante um Evento de Contingência ou Desastre, os colaboradores são orientados a ligar ou contatar um dos contatos listados na lista de emergência disposta na intranet da Empresa.

5.3 Procedimentos após Evento de Contingência ou Desastre

Na ocorrência de um Evento de Contingência ou Desastre, será estabelecido um comitê de gerenciamento de crise (“**Comitê de Gerenciamento de Crise**”), composto essencialmente pela Atual-IT, Diretora de Gestão de Risco e um colaborador nomeado em conjunto por ambos, os quais ficarão responsáveis por:

- avaliar os impactos diretos e indiretos sofridos;
- elaborar e implementar um plano de ação para recuperação dos serviços impactados, em especial com vistas a restabelecer as 4 funções críticas à Empresa, com a maiorbrevidade possível;
- comunicar aos demais Colaboradores acerca do referido plano de ação e se necessário, convocá- los para reunião presencial para esclarecimento de dúvidas e ponderações acerca das medidas que foram e serão adotadas em tal cenário; e
- atuar para a reparação da estrutura afetada, incluindo, mas não se limitando, conforme o caso, ao reestabelecimento do ambiente, dos sistemas de rede e operacionais, bem como estabelecer metodologias de prevenção à ocorrência de novos eventos de contingência ou desastre com características similares (se e quando possível) mitigando, destaforma, o risco de recorrências.

O Comitê de Gerenciamento de Crise será instaurado e permanecerá atuante até que sanados todos problemas decorrentes do Evento de Contingência ou Desastre e restabelecidas, em sua integralidade, as funções e atividades da Empresa.

6 Registros, Treinamentos & Revisões Periódicas

6.1 Registros de Ocorrências

Caberá ao Comitê de Gerenciamento de Crise o registro em pauta de toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste plano. Constará de tal registro, no mínimo:

- Descrição dos fatos;
- Data e hora (quando aplicável) da ocorrência;
- Descrição das medidas adotadas;
- Data e hora (quando aplicável) do reestabelecimento das condições normais detrabalho;
- Informações adicionais (eventualidades, estragos e afins); e
- Assinaturas da Diretora de Gestão de Risco e da Atual-IT.

As pautas de registro ficarão armazenadas com a Diretora de Gestão de Risco pelo prazo de cinco anos.

6.2 Treinamentos Periódicos

Todos os Colaboradores comparecerão a um treinamento anual sobre o presente Plano de Contingência (e quando necessário, a reuniões adicionais sobre o tema), que se dará conjuntamente com a reunião anual de treinamento de *Compliance*. Tal treinamento será elaborado e apresentado pela Atual-IT sob supervisão da Diretora de Gestão de Risco.

6.3 Revisões Periódicas

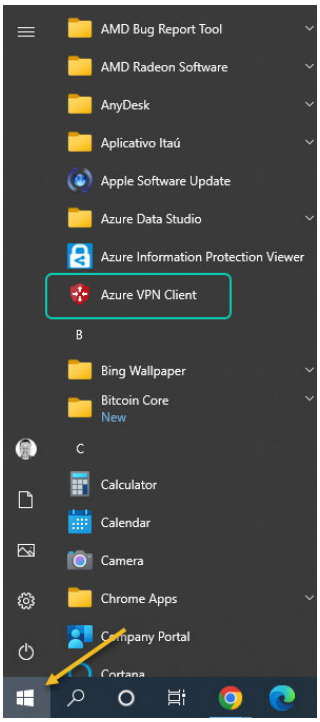
O presente Plano de Contingência será revisado anualmente pela Atual-IT ou, quando necessário, na ocorrência de alterações nos processos ou na estrutura adotados pela M Square (seja por otimização, adequações, ou introdução de novas tecnologias) e estará sujeito à validação pela Diretora de Gestão de Risco da M Square. O Plano de Contingência será também testado, conforme a regulação aplicável, com o objetivo de avaliar se o Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da M Square e de manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se pode ser ativado tempestivamente.

Todos os Colaboradores receberão uma cópia do presente Plano de Contingência, além do treinamento anual mencionado acima, e poderão acessá-lo, em sua versão mais atual, a qualquer tempo, no website da Empresa.

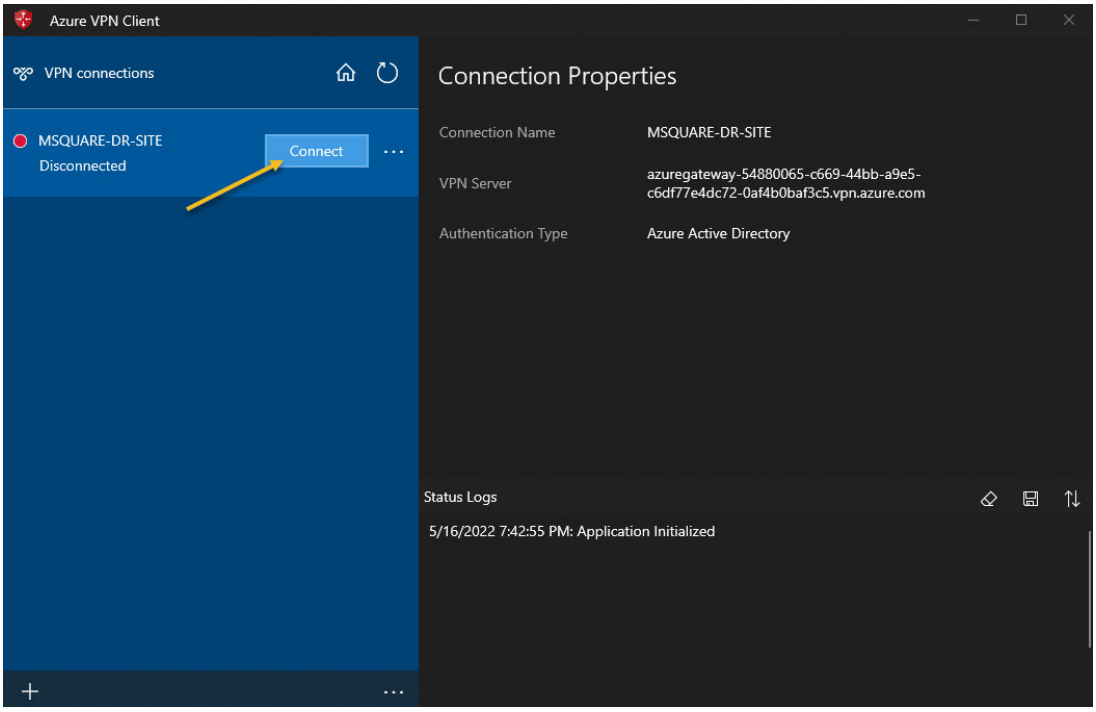
Acesso ao ambiente de DR – Notebooks Corporativos

O acesso deve ser feito através de um notebook corporativo:

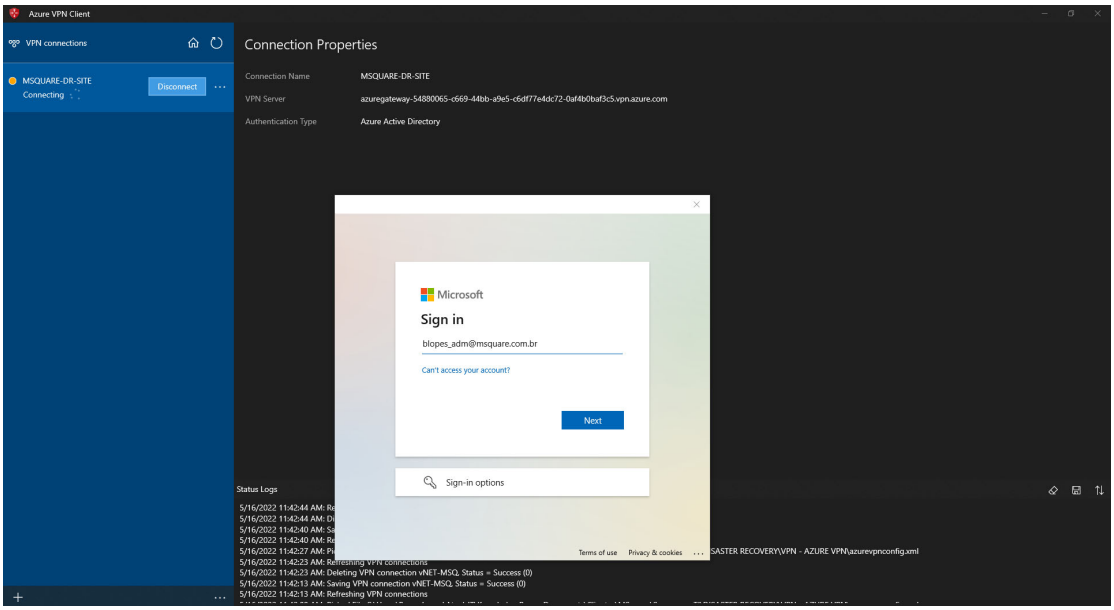
1. Clicar no menu “iniciar” -> “Azure VPN”

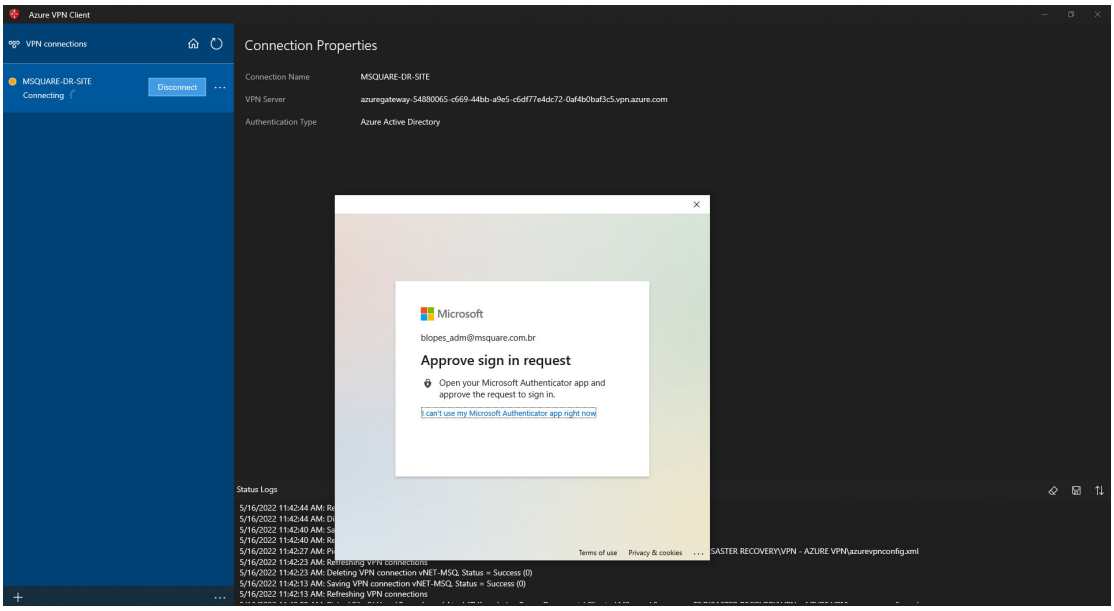


2. Dentro do “Azure VPN Client” selecione a conexão “MSQUARE-DR-SITE” e clique em “Connect”

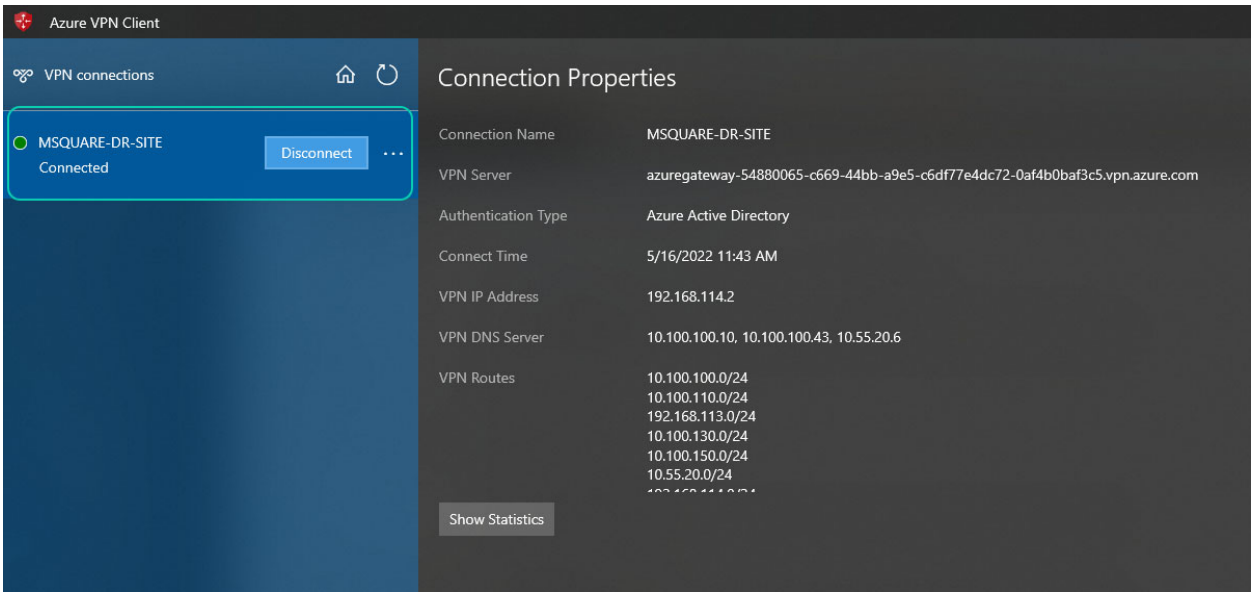


3. Será solicitado a autenticação do usuário. Coloque seu email@msquare.com.br, senha e depois aprove o MFA


Azure VPN Client
VPN connections
MSQUARE-DR-SITE
Connecting
Disconnect
Connection Properties
Connection Name
MSQUARE-DR-SITE
VPN Server
azuregateway-54880065-c669-44bb-a9e5-c6df77e4dc72-0af4b0baf3c5.vpn.azure.com
Authentication Type
Azure Active Directory
Microsoft
Sign in
blopes_adm@msquare.com.br
Can't access your account?
Next
Sign-in options
Terms of use
Privacy & cookies
Status Logs
5/16/2022 11:42:23 AM: Deleting VPN connection vNET-MSQ, Status = Success (0)
5/16/2022 11:42:13 AM: Saving VPN connection vNET-MSQ, Status = Success (0)
5/16/2022 11:42:13 AM: Refreshing VPN connections


Azure VPN Client
VPN connections
MSQUARE-DR-SITE
Connecting
Disconnect
Connection Properties
Connection Name
MSQUARE-DR-SITE
VPN Server
azuregateway-54880065-c669-44bb-a9e5-c6df77e4dc72-0af4b0baf3c5.vpn.azure.com
Authentication Type
Azure Active Directory
Microsoft
blopes_adm@msquare.com.br
Approve sign in request
Open your Microsoft Authenticator app and approve the request to sign in.
I can't use my Microsoft Authenticator app right now
Terms of use
Privacy & cookies
Status Logs
5/16/2022 11:42:23 AM: Deleting VPN connection vNET-MSQ, Status = Success (0)
5/16/2022 11:42:13 AM: Saving VPN connection vNET-MSQ, Status = Success (0)
5/16/2022 11:42:13 AM: Refreshing VPN connections

4. A conexão será estabelecida e o acesso aos servidores do DR estarão disponíveis.



ANEXO VIII

POLÍTICA DE CERTIFICAÇÃO CONTINUADA DE COLABORADORES

1 Objetivo

O objetivo desta Política de Certificação Continuada de Colaboradores ("Política") é estabelecer os procedimentos que deverão ser seguidos pela M Square e seus Colaboradores, de maneira a buscar a permanente observância ao Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA") e demais normativos aplicáveis, em especial o controle das certificações exigidas e seus respectivos prazos.

2 Áreas Responsáveis

O processo de seleção, admissão e desligamento e *checklist* dos profissionais para a M Square é realizado conforme os termos da "Política de Seleção e Contratação de Colaboradores".

A necessidade de contratação de um profissional com certificação é demandada pelo gestor da área elegível à certificação e informado à área Administrativa e de *Compliance*.

A área de *Compliance* adotará os procedimentos formais de controle, passíveis de verificação, relacionados à obtenção e expedidas pelo Código ANBIMA, bem como se o controle de admissão e desligamento de Colaboradores manutenção da certificação ou isenções pertinente a todos os seus profissionais, de acordo com as diretrizes específicas está funcionando adequadamente e, ainda, se tais eventos estão sendo devidamente atualizados no banco de dados da ANBIMA, quando aplicável.

A área Administrativa será também responsável por monitorar o prazo de vencimento da certificação ou isenção daqueles Colaboradores que necessitam dela para exercer sua atividade.

Este monitoramento também será realizado através dos respectivos eventos do sistema de gerenciamento de *Compliance* da Gestora (sistema Compli.ly®).

3 Áreas elegíveis e certificações necessárias

Dentre as diversas áreas da M Square, a área de gestão é a única elegível à certificação por desempenhar atividades de gestão profissional de recursos de terceiros ("Atividade Elegível").

A certificação mínima exigida para os gestores (profissionais que atuam na Gestão de Recursos de Terceiros e que têm alçada/poder discricionário de investimento, compra e venda, dos ativos financeiros integrantes das carteiras dos Veículos de Investimento) é o CGA, salvo exceções previstas na regulamentação.

Os analistas que exercem atividades de apoio à área de gestão não são elegíveis a certificação por não desempenharem as atividades acima mencionadas.

Caso a M Square venha a atuar em outras áreas que demandem certificação, essa Política deverá ser alterada, de forma a incluir essa área entre as Áreas Elegíveis.

4 Procedimento de identificação de profissionais certificados

Na definição da necessidade de um novo integrante/substituição, o responsável pela área contratante deverá informar à área de *Compliance* se há necessidade de certificação.

Em caso positivo, este aspecto já deve ser levado em consideração na triagem dos candidatos. Em caso negativo, quando da admissão de qualquer Colaborador deverá ser questionado se ele detém alguma certificação ou isenção perante à ANBIMA.

Em sendo certificado ou isento, mesmo que para cargo não elegível, o novo Colaborador deverá ser atualizado junto ao Banco de Dados da ANBIMA, conforme as regras aplicáveis.

5 Mudança de colaborador entre área elegível ou não elegível

Com controle efetuado pela Gestora, a área de *Compliance* mapeará todos os Colaboradores certificados ou isentos ou não, as áreas de atuação e a necessidade de certificação.

Na ocorrência de mudança de área de um profissional certificado ou isento para uma área não elegível à certificação, a Diretora responsável pela área elegível deverá manter um substituto devidamente certificado ou isento para a respectiva atividade.

No caso de um profissional não certificado se candidatar a um cargo elegível, este deverá buscar a certificação ou isenção elegível antes de assumir o referido cargo.

O monitoramento de todos os procedimentos acima cabe à área de *Compliance*, em conjunto com a área Administrativa.

6 Licenciamento de profissional certificado

O responsável pela área elegível deverá manter, ao menos, um substituto devidamente certificado ou isento apto para assumir as funções do cargo em vacância.

7 Controle dos prazos das certificações e notificações

A área de *Compliance* tem mecanismos internos de alerta de vencimento de certificação ou isenção, com o objetivo de acompanhar as datas de vencimento, realizando revisões do controle trimestralmente e o mantendo atualizado no sistema de gerenciamento de *Compliance* da Gestora (sistema Compli.ly®).

De acordo com o Código ANBIMA, a atualização das certificações e isenções ANBIMA devem seguir a seguinte regra para atualização:

I. CGA para Profissional Certificado ou Profissional Isento vinculado à Gestora:

(i) Caso esteja exercendo a Atividade Elegível e a certificação não esteja vencida: prazo indeterminado;

(ii) Caso não esteja exercendo a Atividade Elegível: 3 (três) anos, contados da data de aprovação no exame, ou da data em que deixar de exercer a Atividade Elegível; ou

II. CGA para profissional aprovado[7] ou profissional isento não vinculado: três anos, contados da data de aprovação no exame ou, da concessão da isenção, ou, ainda, da data que a instituição comunicar a ausência de vínculo no Banco de Dados.

Os profissionais que possuem certificação e isenções cujos vencimentos ocorrerão em até 6 (seis) meses[8] da consulta na base de dados serão informados pela área de *Compliance* para providenciarem a renovação dentro de um prazo adequado sem comprometer as atividades desenvolvida.

---

[7] Pela regulamentação aplicável, profissional aprovado seria aquele com certificação não vencida, porém não vinculado a uma instituição. Tal profissional passa a ser certificado a partir de novo vínculo, a ser realizado no Banco de Dados da ANBIMA, desde que sua certificação não esteja vencida na data do vínculo. Na mesma linha, o profissional certificado terá sua condição alterada para profissional aprovado a partir da data de desligamento informada no Banco de Dados da ANBIMA, desde que a certificação não esteja vencida. No caso de alteração da condição do profissional, as regras específicas sobre a respectiva alteração do prazo de vencimento do Código ANBIMA deverão ser observadas.

[8] Importante notar que as inscrições nos exames para os profissionais certificados ou aprovados poderão ser feitas, apenas, a partir de seis meses do vencimento da referida certificação ou aprovação.

Adicionalmente, a Diretora responsável pela área elegível também receberá uma comunicação sobre os profissionais que estão com os certificados próximos aos vencimentos para acompanhamento e providências junto ao profissional.

O profissional elegível que não regularizar a renovação de sua certificação ou isenção até a data de vencimento será informado pela Diretora responsável que ficará afastado da respectiva Atividade Elegível, e passará a atuar apenas em atividades de apoio. Nesse caso, o Colaborador receberá um e-mail da área de *Compliance* sobre o afastamento e terá suas senhas de acesso aos sistemas de negociação e às corretoras bloqueados, até a obtenção da sua devida atualização. O afastamento também será controlado no sistema de gerenciamento de *Compliance* da Gestora (sistema Compli.ly®).

Na hipótese mencionada acima, tal Colaborador somente retomará suas atividades após a devida regularização da certificação e envio de comprovação à área de *Compliance* para atualização junto ao Banco de Dados ANBIMA. Após a devida atualização, a área de *Compliance* comunicará, a Diretora responsável pela área elegível, que o profissional afastado está devidamente regularizado junto a ANBIMA, e poderá voltar à Atividade Elegível.

Para todos os profissionais certificados ou isentos que atuem em área elegível ou não-elegível é solicitado que regularizem a referida certificação ou isenção assim que estiver disponível pela ANBIMA a execução das respectivas provas.

Para os profissionais que, eventualmente, se encontrarem em licença, a área de *Compliance* enviará uma notificação para o e-mail pessoal do Colaborador informando o profissional que, até a regularização da pendência, não poderá exercer as Atividades Elegíveis ao retornar.

A área de *Compliance* acompanhará juntamente com o responsável da área elegível a regularização do profissional e trimestralmente fará o acompanhamento dos prazos por meio do sistema de gerenciamento de *Compliance* (sistema Compli.ly®).

8 Atualização do banco de dados da anbima

A área de *Compliance* deverá incluir no Banco de Dados da ANBIMA as informações cadastrais relativas aos seus Colaboradores certificados ou isentos, em processo de certificação ou isenção, quando esta estiver vencida e/ou em processo de atualização. As informações abaixo deverão, necessariamente, ser incluídas no Banco de Dados da ANBIMA e/ou outras adicionais conforme regulamentação aplicável:

- Data de admissão;
- Data de desligamento, quando aplicável;
- Atividade exercida;
- Área de atuação;
- Cargo;
- Tipo de gestor, quando aplicável; e
- Endereço eletrônico individual.

Ainda, é de responsabilidade da área de *Compliance* a manutenção atualizada do Banco de Dados ANBIMA, devendo atender aos termos e prazos estipulados pela regulamentação, promovendo a atualização das informações do respectivo Banco de Dados até o último dia do mês subsequente considerando a data do evento e/ou de acordo com prazo estabelecido na regulamentação[9].

A atualização ocorre nas seguintes ocasiões e/ou outras que sejam previstas na regulamentação aplicável:

(i) no momento da admissão/desligamento do profissional;

(ii) quando o profissional é certificado ou isento mesmo que em área não elegível após contratação (inclusive quando estiver vencida e/ou em processo de atualização); e

(iii) no momento em que o profissional certificado ou isento é afastado ou retorna de licença.

9 Disposições Gerais

Eventuais dúvidas acerca das diretrizes desta Política poderão ser esclarecidas diretamente com a área de *Compliance*.

[9] A atualização da certificação deve ser informada no Banco de Dados até o último dia do mês subsequente à data da conclusão do treinamento, quando este for oferecido pela Gestora. Se o treinamento for feito pela ANBIMA, a atualização será informada pela própria Associação em até trinta dias da data da conclusão do curso, o que será monitorado pela Gestora.

ANEXO IX

POLÍTICA DE SELEÇÃO, CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

1 Objetivo

Esta Política de Seleção, Contratação e Monitoramento de Terceiros ("Política") tem como objetivo estabelecer os princípios que regem o processo de contratação de prestadores de serviços e fornecedores da M Square agindo em nome dos fundos de investimentos ("Terceiro"). Por meio do desenvolvimento desta Política, a Gestora busca atender às regras previstas nas normas vigentes, em especial no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código Anbima").

Ainda, os processos definidos nesta Política visam mitigar riscos de pagamentos ilícitos, e propiciar à Gestora os meios aptos a rescindir os contratos sempre que houver violação às regras aqui previstas.

2 Responsabilidades

Para fins de cumprimento desta Política, é dever de todos os Colaboradores da Gestora:

- Priorizar os interesses dos fundos de investimento em todas as transações de contratação de serviços de Terceiros, garantindo a boa utilização dos recursos contratados, em especial nos casos em que haja ligação direta ou indireta entre o contratado e demais prestadores de serviços dos fundos, ou investidores na hipótese de potenciais conflitos de interesse;
- Reportar à área de *Compliance* acerca da existência de conflito de interesse em relação ao produto ou serviço em análise, inclusive sua eventual relação de parentesco ou amizade com o fornecedor em tela, ou seu conhecimento acerca do relacionamento entre o Terceiro e o investidor;
- Caso a M Square venha a contratar corretoras, deverá observar adicionalmente aos procedimentos para contratação de corretoras, conforme os procedimentos definidos na Seção 8, Operações e Melhor Execução, deste Manual, bem como observar os procedimentos para contratação de Terceiros quando os fundos de investimento realizam investimentos no exterior, conforme Política de Decisão de Investimentos e de Seleção e Alocação de Ativos e Investimentos no Exterior (Anexo V), mais especificamente no item 4.2 do Anexo V; e

- Zelar ao contratar Terceiros que pertençam ao seu Conglomerado ou Grupo Econômico, ou ao Conglomerado ou Grupo Econômico dos investidores dos fundos de investimento, para que as operações observem condições estritamente comutativas.

A critério da área de *Compliance*, a aplicação das regras previstas nesta Política aos Terceiros deverá observar o porte do Terceiro contratado, o volume de transações, bem como a criticidade da atividade, buscando agir com razoabilidade e bom senso.

3 *Due Diligence* Inicial – *Know Your Partner* - KYP

Desde o início das tratativas, quaisquer Terceiros com os quais a Gestora tenha interesse em realizar negócios e, que desenvolvam atividades consideradas de Risco Alto, para os fundos de investimento, devem passar por um processo de verificação acerca de sua idoneidade, proporcional ao nível de risco do contrato a ser celebrado, a critério da área de *Compliance*/Jurídica.

Determinados Terceiros contratados podem ser chamados a aderir determinadas Políticas da Gestora, e assinar acordos de confidencialidade (que pode ser por meio eletrônico), caso tenham acesso a informações confidencias da Gestora, seus fundos de investimento ou investidores, a critério da área de *Compliance*/Jurídica.

3.1 Processo de Avaliação do Prestador de Serviço e Análise de Mercado

A *due diligence* inicial consiste no processo de verificação prévia dos dados da empresa e seus sócios, anteriormente ao início de qualquer vínculo, seja por meio da análise de informações públicas disponibilizadas na internet ou, ainda, diretamente solicitadas aos Terceiros.

A fase inicial será realizada pelo departamento responsável pelo contrato (área demandante), e seguirá conforme os parâmetros mínimos estabelecidos pela área de *Compliance*/Jurídica, conforme disposto no Anexo A a esta Política.

Em seu processo de contratação de Terceiros, a Gestora exigirá que o Terceiro responda ao questionário ANBIMA de *Due Diligence* específico para a atividade contratada, quando aplicável, conforme modelos disponibilizados pela ANBIMA em seu site na internet, sem prejuízo da solicitação de informações adicionais a critério da Gestora, dependendo da classificação de risco do Terceiro, conforme item 6 abaixo.

Nos casos de contratação de Terceiros para atividades autorreguladas pela ANBIMA que não possuam questionário ANBIMA de *Due Diligence*, a Gestora deverá observar procedimento interno

adicional, com a utilização de seu questionário próprio (sendo certo que se o Terceiro não for aderente aos Códigos da ANBIMA aplicáveis à sua respectiva atividade será considerado de Alto Risco, conforme classificação do item 6 abaixo.

O processo de decisão de contratação de serviço deve levar em consideração, entre outros aspectos, qualidade, expertise, preço, custo, vida útil do produto/serviço, obsolescência, fluxo de caixa e orçamento, de acordo com o caso. Ademais, especificidades sobre cada tipo de prestador de serviços e os critérios que fazem a Gestora decidir por um Terceiro em detrimento do outro estão dispostos na Seção 8, Operações e Melhor Execução, deste Manual .

O início das atividades do Terceiro deve ser vinculado à formalização da contratação, e nenhum tipo de pagamento poderá ser efetuado antes da celebração do respectivo contrato.

4 Processo de aprovação do prestador de serviço

Todo processo de contratação de serviços deve ser previamente aprovado pelo/a Diretor/a responsável pela área que demandou a contratação (área demandante / gestor do contrato) e, em seguida pela área de *Compliance*/Administrativa que irá coordenar o processo. Da mesma forma, todos os pagamentos relacionados à contratação de serviços devem ser sempre aprovados através da assinatura/autorização de duas pessoas autorizadas da Gestora (entende-se por pessoa autorizada aquelas que possuam acesso ao sistema de pagamentos da Gestora com autorização para aprovar pagamentos).

5 Formalização contratual e cadastro

As regras para formalização do contrato e cadastro do Terceiro deverão ser estabelecidas pela área de *Compliance*, de acordo com o nível de risco do contrato (vide item 6 abaixo), sobretudo em termos de sensibilidade de informações a serem transmitidas durante o relacionamento contratual, avaliando: (i) se o serviço poderá impactar os fundos de investimento; (ii) se as condições de ruptura contratual estão bem dimensionadas e eventual rescisão não impactará a Gestora; (iii) existência de cláusula de confidencialidade e anticorrupção, dentre outros aspectos que se fizerem necessários para o caso concreto.

Deverá ser mantida arquivada sob responsabilidade da área de *Compliance*/Administrativa por período não inferior a 5 (cinco) anos toda a documentação do processo de seleção de prestadores de serviço, incluindo os orçamentos recebidos (quando aplicável), as características técnicas do

serviço, garantias, a aprovação do/a Diretor/a da área demandante, serviço de manutenção, recargas, e-mail, recibos e notas de compra e quaisquer outros documentos que se mostrarem relevantes.

As obrigações e condições tratadas por telefone deverão ser formalizadas por e-mail, de forma a manter histórico das decisões tomadas e eventuais conflitos existentes.

O contrato celebrado pela Gestora ou em nome dos fundos de investimento deve conter no mínimo as cláusulas listadas no Anexo A à presente.

6 Classificação de riscos de terceiros baseada em risco

A área de *Compliance* da Gestora é responsável por realizar avaliações periódicas, em período não superior a 36 (trinta e seis) meses dos Terceiros contratados, de acordo com a classificação de risco do Terceiro (exclusivamente aqueles que desenvolvam atividades para os fundos de investimento).

A supervisão baseada em risco tem como objetivo destinar maior atenção aos Terceiros contratados que demonstrem maior probabilidade de apresentar falhas em sua atuação ou representem potencialmente um dano maior para os investidores e para a integridade do mercado financeiro e de capitais. A Gestora desenvolveu a seguinte classificação interna de risco:

- **Risco Baixo**: Terceiros cuja atividade não gera riscos estratégicos, legais/de *Compliance*, operacionais, financeiros/de crédito ou reputacionais para a Gestora.
- **Risco Médio**: Terceiros cuja atividade gera ao menos um dos riscos acima apontados, ou tenham acesso à informações confidenciais dos fundos de investimento ou investidores, mas que demonstram procedimentos e controles aparentemente satisfatórios, quando da resposta do questionário de *due diligence*, tendo em vista que a Gestora não realizará testes para confirmar a efetividade dos controles, tampouco é responsável pela gestão desses controles. A avaliação será feita apenas por meio da declaração dos Terceiros em questionários e/ou conversas, reuniões e entrevistas.
- **Risco Alto**: Terceiros cuja atividade gera ao menos um dos riscos acima apontados, e que não são capazes de demonstrar a existência de controles e/ou que apresentam problemas cuja natureza pode trazer responsabilidade/implicações à Gestora, como no caso de Terceiros que já foram envolvidos em escândalos de corrupção, lavagem de dinheiro, ou que estão

sendo processados ou investigados pela prática de algum ato relacionado a sua atividade ou a atividade a ser prestada à Gestora.

Terceiros que não sejam Associados ou Aderentes aos Códigos Anbima, ou que, exercendo atividade autorregulada pela ANBIMA, não possuam questionário de DDQ padrão ANBIMA serão automaticamente classificados como Alto Risco. Para esses Terceiros, a área de *Compliace* deverá adotar critérios adicionais para supervisão conforme tabela abaixo, e estes deverão ser supervisionados, no mínimo, a cada doze meses.

Com base na classificação acima, a Gestora deverá desenvolver lista com os prestadores de serviços/ fornecedores contratados, e sua classificação de risco interna, a qual deverá ser mantida atualizada pela área de *Compliance*/Jurídica da Gestora, através do sistema Compli.ly® utilizado pela Gestora.

7 Monitoramento dos prestadores de serviço baseado em risco – revisões periódicas

Atividades de Controle	**Risco baixo**	**Risco médio**	**Risco alto**
Questionários de *due diligence*	x	x	x
Obrigação de confidencialidade		x	x
Revisão de contratos (cláusulas mínimas)	x	x	x
Background search		x	x
Avaliação de *Compliance*	x	x	x
Entrevistas		x	x
Revisão *on-site*			x
Monitoramento dos pagamentos realizados	x	x	x
Término do contrato (a ser avaliado)			x

Periodicidades mínimas para revisões dos Terceiros

Risco Baixo: 36 meses

Risco Médio: 24 meses

Risco Alto: 12 meses

Não obstante a periodicidade definida acima, caso se verifiquem fatos novos relativos ao negócio ou a pessoa do Terceiro, como por exemplo alterações no escopo da contratação inicial, a critério da área de *Compliance*, deverá ser conduzida reavaliação do Terceiro, em razão de tais fatos, mesmo antes da periodicidade aqui mencionada.

Caso se verifique mudanças significativas nas condições previstas no processo de *due diligence*, estes poderão ter seu contrato rescindido, conforme decisão do Comitê de Risco e *Compliance*. A área de *Compliance* deverá formalizar em relatório próprio, para posterior encaminhamento aos órgãos de administração da Gestora ou, no caso de identificação de qualquer descumprimento, para tomada das providências necessárias.

8 Contratação de empresas do grupo da gestora

Podem ser dispensados das obrigatoriedades previstas nessa Política as empresas que pertençam ao mesmo grupo econômico da Gestora. Nestes casos, será necessário apenas que seja firmado acordo ou contrato formal entre as partes.

9 Não conformidades & gestão de crises

Em caso de identificação de não conformidades no relacionamento contratual ou, se a qualquer momento do relacionamento, o Terceiro seja envolvido em operações relacionadas à corrupção, fraude a licitação, suborno, ou qualquer outro crime ou ilícitos administrativos, a área de *Compliance*/Jurídica (i) determinará à área demandante / gestor do contrato o encerramento imediato do relacionamento mediante envio de notificação de rescisão contratual; e (ii) fará levantamento do histórico do Terceiro junto à Gestora e elaborará dossiê sobre o caso para o Comitê de Risco e *Compliance*, que decidirá sobre as medidas legais e regulatórias que serão tomadas pela Gestora, incluindo notificação às autoridades competentes.

ANEXO A

GUIA DE PROCEDIMENTOS PARA REALIZAÇÃO DE *DUE DILIGENCE* INICIAL E FORMALIZAÇÃO DE CONTRATO E CADASTRO DA GESTORA.

Os procedimentos abaixo listados são recomendados quando da contratação de qualquer Terceiro de Risco Medio ou Alto, que desenvolva atividade diretamente relacionada ao *core business* da Gestora.

1. *Due Diligence* Inicial

- Cópia do cartão de CNPJ, obtido no site da Receita Federal e QSA/Capital Social;
- Data de início das atividades;
- Pesquisas na internet para verificar se há informações desabonadoras sobre a empresa, seus sócios e administradores, consultando, em especial, o site do Portal da Transparência do Governo Federal, que contém o Cadastro Nacional de Empresas Inidôneas e Empresas Punidas;
- Se necessário, consultar banco de dados do SERASA/SPC; e
- Se necessário, consultar os sites dos tribunais de justiça de cada estado/justiça federal, Tribunal Superior do Trabalho, Superior Tribunal de Justiça, Superior Tribunal Federal.

A área demandante da contratação e a área de *Compliance* poderão solicitar informações adicionais relativas ao Terceiro, seus sócios e administradores, caso julgue necessário ou conveniente para melhor avaliar o Terceiro.

A critério da área de *Compliance*, os procedimentos listados acima podem ser dispensados ou acrescidos de mais providências, conforme o caso, desde que devidamente justificado por escrito.

2. Formalização de Contrato e Cadastro

Questionário de DDQ ANBIMA próprio para atividade do Terceiro /Modelo de DDQ próprio Gestora, conforme o caso;

Via física ou digital do contrato, devidamente assinada por todas as partes.

Cópia das Políticas de Ética e Conduta e Anticorrupção do Terceiro (dentre outras Políticas relevantes ao serviço que venha a ser contratado).

Ademais, a área demandante da contratação e a área Jurídica/de *Compliance* deverão envidar melhores esforços para avaliar, durante o processo de contratação:

Os Colaboradores envolvidos na contratação também deverão envidar seus melhores esforços para verificar e confirmar as informações recebidas do Terceiro.

Cláusulas mínimas de qualquer contrato celebrado pela Gestora e em nome dos fundos de investimento:

I. As obrigações e deveres das partes envolvidas;

II. A descrição das atividades que serão contratadas e exercidas por cada uma das partes;

III. A obrigação de cumprir suas atividades em conformidade com as disposições previstas neste Código e na Regulação em vigor específica, no que aplicável, para cada tipo de fundo de investimento; e

IV. Que os Terceiros contratados devem, no limite de suas atividades, deixar à disposição do Administrador Fiduciário todos os documentos e informações exigidos pela Regulação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da Regulação em vigor.

ANEXO X
POLÍTICA DE PRIVACIDADE E SEGURANÇA CIBERNÉTICA

A Política de Privacidade e Segurança Cibernética ("Política") tem por objetivo estabelecer as regras, procedimentos e controles visando assegurar a segurança cibernética da M Square, ("Gestora") bem como a confidencialidade, integridade, privacidade e disponibilidade dos dados e dos sistemas de informação utilizados pela Gestora. Esta Política de Privacidade e de Segurança da Informação ("Política") é uma declaração formal da empresa acerca de seu compromisso com a privacidade e a proteção das informações de sua propriedade e/ou sob sua guarda.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo a Lei nº 13.709/18 – Lei Geral de Proteção de Dados ("LGPD"), o Código ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros e o Guia de Cibersegurança de dez/2017, bem como as boas práticas de mercado.

1 Responsabilidade

1.1 Responsável pelo Programa de Governança em Privacidade e pela Segurança Cibernética

O(A) Diretor(a) de *Compliance* é responsável por esta Política, sendo o principal contato dentro da Gestora para tratar e responder questões de privacidade e segurança cibernética ("Responsável pela Segurança Cibernética e DPO"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Os deveres e responsabilidades do(a) Diretor(a) de *Compliance*, na qualidade de Responsável pela Segurança Cibernética e DPO, incluem, dentre outros:

- Testar a eficácia dos controles (como por exemplo, backup e controle de infraestrutura) utilizados e informar ao Comitê de Privacidade e Segurança Cibernética os riscos residuais.
- Elaborar as políticas internas de segurança da informação e de proteção da privacidade e suas atualizações, garantindo mecanismos eficazes de monitoramento.
- Responder solicitações de Investidores, Colaboradores, terceiros e autoridades relacionadas à LGPD, podendo contar com o apoio de outros Colaboradores.
- Direcionar esforços e recursos propostos para a segurança da informação e a proteção da privacidade.
- Assegurar que seja realizada a configuração dos equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os

requerimentos de segurança estabelecidos por esta Política, bem como definir e assegurar a segregação das funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Gestora.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Gestora.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Gestora, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Gestora.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Gestora operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Propor as metodologias e os processos específicos para a segurança da informação e para a proteção de Dados Pessoais sob responsabilidade da M Square, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Gestora.
- Garantir um backup em nuvem, devidamente criptografado com as rotinas de retenção (2 últimas semanas / cabeça de mês / cabeça de ano – por 5 anos).
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação e da proteção de Dados Pessoais para o negócio da Gestora, mediante campanhas, treinamentos e outros meios de endomarketing.

Garantir que Parceiros, Fornecedores e Prestadores de serviços externos mantenham programas de Governança em Privacidade e pela Segurança Cibernética.

1.2 Comitê de Privacidade e Segurança Cibernética

O Comitê de Privacidade e Segurança Cibernética será composto pela equipe de *Compliance*, a qual poderá sempre que julgar necessário, convidar outros membros da área de TI para compor o respectivo comitê.

Ressaltamos que o Comitê de Privacidade e Segurança Cibernética ocorrerá dentro do Comitê de *Compliance* da M Square e se reunirá sempre que necessário para deliberar, além das matérias indicadas no Item 1.1 acima, sobre:

- Definição e revisão de quaisquer regras, normas e procedimentos internos adotados pela Gestora para o cumprimento das responsabilidades e obrigações listadas no item 2 desta Política, incluindo a constituição de manuais internos complementares desta Política.
- Avaliação dos riscos internos e externos, (*risk assessment*) identificados nos termos do item 4 desta Política.
- Estabelecer ações de prevenção, proteção e medidas internas em prevenção a ocorrência de ataque cibernético nos termos do item 5 desta política.
- Análise dos procedimentos de monitoramento e de testes periódicos nos termos do item 6 desta Política.
- Cumprimento Plano de Resposta a Incidentes quando o Responsável pela Segurança Cibernética e DPO tenha sido acionado devido a um potencial incidente envolvendo risco cibernético e/ou questões de privacidade, nos termos do item 6 desta Política.

1.3 Atribuições de Todos os Colaboradores

Caberá a todos os Colaboradores conhecer e adotar as definições desta Política, e seus deveres e responsabilidades na manutenção da segurança corporativa e da privacidade. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança cibernética ou a proteção de dados pessoais, o qual recorrerá a(o) Diretor(a) de *Compliance*, se for o caso.

Em caso de qualquer incidente que afete a privacidade e/ou a segurança cibernética da Gestora, ou dos prestadores de serviços e parceiros externos, ou a observância de descumprimento desta Política, o Colaborador deverá comunicar imediatamente a(o) Diretor(a) de *Compliance* e/ou a Área Administrativa

Em caso de descumprimento, ainda que involuntário, o Colaborador responsável poderá estar sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei, a exclusivo critério da Gestora.

2 Proteção da Privacidade e de Dados Pessoais

Este capítulo tem o objetivo de esclarecer as características, regras e finalidades do tratamento de dados pessoais realizados pela M Square para a prestação de seus serviços de gestão profissional de recursos de terceiros com foco em investimentos e produtos internacionais ("Serviços").

Os Colaboradores, Investidores e clientes, parceiros, fornecedores e prestadores de serviços terceiros todos deverão compreender e aceitar guiar-se por esta Política. Caberá a M Square a responsabilidade de comunicação e divulgação das regras e procedimentos adotados para cada público sujeito a Política.

A M Square poderá alterar esta Política a qualquer tempo por meio de atualização publicada no Website, à qual você ficará vinculado.

2.1 O que são Dados Pessoais?

A lei define como "dado pessoal" qualquer informação relacionada a uma pessoa natural identificada ou identificável. Tal pessoa é o "titular" dos dados.

Alguns dados pessoais são considerados "sensíveis", recebendo maior proteção legal, dentre eles os de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.

O tratamento de dados inclui toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2.2 De que forma a M Square coleta Dados Pessoais?

A M Square coleta dados pessoais:

- de Investidores e clientes, de seus representantes e de potenciais clientes, fornecidos por escrito por meio de documentos de subscrição, questionários, documentos, ou, ainda, pessoalmente, por telefone ou via e-mail;
- via recebimento e transferência de dados para parceiros, fornecedores e prestadores de serviços ("Parceiros");
- de potenciais candidatados a vagas internas, fornecidos durante o processo de recrutamento; e/ou
- de Colaboradores fornecidos no processo de admissão.

2.3 Quais dados são tratados pela M Square e por quê?

A M Square realiza o tratamento dos dados pessoais, sobretudo, para a execução e melhoria dos Serviços, cumprimento de obrigações regulatórias e execução dos contratos de que é parte.

Como regra, a M Square não solicita dado pessoal sensível ou de indivíduos menores de 18 anos para a realização dos Serviços. É possível que alguns dados pessoais sensíveis sejam coletados em caso específicos, tal como de Colaboradores ou de seus dependentes para fins regulatórios. Desta forma, nenhuma informação desta natureza deve ser fornecida à M Square a não ser que expressamente solicitada. Caso sejam fornecidos dados pessoais sensíveis por engano ou imprudência, será interpretado que o titular dos dados pessoais autorizou expressamente a M Square a eliminar ou anonimizar tais dados.

2.4 Como ocorre o compartilhamento de Dados Pessoais?

A M Square compartilha dados pessoais com Parceiros ou Prestadores de Serviços terceiros, desde que previstos em contratos, para aa estrita necessidade para execução dos Serviços, cumprimento de normas e funcionamento da Gestora.

Os serviços prestados pelos Parceiros ou Prestadores de Serviços terceiros são, primordialmente: (i) administração fiduciária de fundos de investimento; (ii) distribuição de cotas fundos de investimento; (iii) custodia de ativos de investimentos; (iv) serviços bancários como manutenção e movimentação de conta corrente (v) contabilidade e folha de pagamento de Colaboradores (vi) serviços de recrutamento e divulgação de vagas; e (vii) serviços de tecnologia e segurança da informação.

Excepcionalmente, a M Square poderá compartilhar Dados Pessoais em outras hipóteses como: (i) responder uma intimação ou ordem judicial, processo judicial ou autoridades regulatórias; (ii) suspeita de conduta potencialmente criminal ou fraudulenta; (iii) interesses legítimos da M Square, mediante prévia anonimização; e/ou (iv) em outras situações excepcionais, mediante consentimento prévio do titular dos dados pessoais.

A M Square não compartilha dados pessoais para fins de marketing e não vende Dados Pessoais sob nenhuma hipótese.

2.5 Transferência internacional de Dados

A M Square realiza transferência internacional de dados pessoais com Parceiros e/ou Prestadores de Serviços terceiros localizados no exterior com o objetivo de viabilizar a prestação dos Serviços e cumprimento de obrigações regulatórias locais. Para isso, a M Square observa todos os requerimentos estabelecidos pela legislação aplicável e adota as melhores práticas de segurança e

privacidade para garantir a integridade e confidencialidade de quaisquer dados pessoais de Investidores.

Cabe a M Square a supervisão e questionamentos sobre políticas e regras adotadas de Governança em Privacidade adotadas nesses casos.

2.6 Eliminação e anonimização de Dados Pessoais dos colaboradores e investidores ou clientes?

A M Square mantém dados pessoais coletados após o término da prestação dos Serviços aos investidores ou clientes e após o desligamento de Colaboradores, conforme aplicável, pelo tempo exigido pela legislação ou regulação aplicável ou para fins de cumprimento de seus deveres e direitos empresariais perante órgãos de supervisão e fiscalização. Em alguns casos, os dados podem ser eliminados ou anonimizados antes do esperado, caso já não sejam mais necessários para finalidade para que foram coletados.

2.7 Direitos do Titular dos Dados Pessoais

Aqueles que fornecem seus Dados Pessoais à M Square, tem os seguintes direitos, desde que não desrespeite a legislação ou regulação aplicável conforme mencionado no item 2.6 acima:

Direitos do Titular	
Acesso	Requerer cópia de ou confirmação de quais são os seus Dados Pessoais sob custódia da M Square.
Correção	Solicitar a correção de seus Dados Pessoais. Para efetivar a correção, a M Square checará a veracidade e titularidade dos dados fornecidos.
Anonimização, bloqueio ou eliminação	Requerer a suspensão temporária de qualquer operação de tratamento de seus Dados Pessoais e solicitar sua exclusão da base de dados da M Square quando entender que são desnecessários ou excessivos.
Portabilidade	Solicitar a transferência de seus Dados Pessoais a outro prestador de serviços, salvo Dados Pessoais já anonimizados ou eliminados pela M Square.
Exclusão	Requerer a exclusão de seus Dados Pessoais tratados com base no consentimento.
Compartilhamento	Ser informado acerca de todas as entidades com as quais seus Dados Pessoais são compartilhados. Para tanto, o titular poderá basear-se nesta Política.
Negativa ou Revogação do consentimento	Não consentir ou revogar seu consentimento acerca do tratamento de seus Dados Pessoais realizado pela M Square, ressalvado os casos em que não é necessário o consentimento para seu tratamento, sendo que o tratamento

	realizado previamente à solicitação continuará válido. Nesse caso, a M Square ficará impossibilitada de fornecer os serviços de comunicação e envio de formulários e newsletters do Website.

Os direitos acima podem ser exercidos mediante solicitação à M Square, a qualquer tempo e por qualquer razão pelo e-mail: Compliance@msquare.com.br.

A M Square alerta que a revogação dos consentimentos expressos nesta Política pode resultar na impossibilidade e inviabilização e continuidade de prestação dos Serviços.

2.8 Cookies

Cookies são pequenos arquivos contendo informações enviados de um Website para o seu navegador, os quais são utilizados principalmente para identificar e armazenar informações.

A M Square utiliza Cookies para tarefas distintas, como oferecer uma navegação eficiente, recolher estatísticas, otimizar as funcionalidades e melhorar a experiência do usuário. A M Square não coleta dados pessoais através de Cookies ou acessos no Website.

O período que o navegador armazena as informações provenientes dos Cookies, dependerá do tipo de Cookie, os quais geralmente possuem uma data de expiração.

Ao continuar navegando no Website, o usuário concorda com a nossa Política de Privacidade e de Segurança Cibernética.

2.9 Sites de terceiros

O Website poderá ter em seu conteúdo links de outros sites, o que não significa que esses sites sejam de propriedade ou operados pela M Square. Ao clicar nestes anúncios ou links e ser direcionado para o site destes anunciantes, deverão ser observadas as políticas e termos do site em questão.

2.10 Dúvidas ou solicitações

Dúvidas e solicitações acerca desta Política devem ser direcionadas a(o) Diretor(a) de *Compliance*, encarregado para os assuntos de LGDP, conforme abaixo:

Nome: Renata Borges da Silveira
Endereço: Av. Brig. Faria Lima, 3355, 10º andar
E-mail: Compliance@msquare.com.br.

3 Princípios da Segurança dos dados e dos sistemas de informação

O objetivo das regras sobre segurança cibernética da Gestora é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança ou ataques cibernéticos e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Gestora devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Gestora, observadas as regras de sigilo da Política de Confidencialidade e Segurança da Informação constante no Manual de *Compliance* e o item sobre confidencialidade no Código de Ética da Gestora.

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela M Square pertence à Gestora. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

A M Square reserva-se ao direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4 Identificação/avaliação de riscos (*risk assessment*)

A M Square periodicamente, no mínimo uma vez ao ano, deverá identificar os riscos internos e externos, bem como os ativos de *hardware* e *software* e processos que precisam de proteção. Esse processo será coordenado pelo Comitê de Privacidade e Segurança Cibernética, o qual deverá ser documentado pelo(a) Diretor(a) de *Compliance* com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Gestora e seus riscos de cibersegurança e de privacidade. A Gestora poderá contratar uma empresa terceirizada para tanto, caso a(o) Diretor(a) de *Compliance* julgue necessário e mediante aprovação do Comitê de Privacidade e de Segurança Cibernética.

Após a condução do referido processo, o Comitê de Privacidade e Segurança Cibernética deverá discutir eventuais falhas e riscos observados e discutir as opções de tratamento e de correção e de adoção de novos processos e controles, na tentativa de eliminar as vulnerabilidades e os riscos, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Segue abaixo uma lista não exaustiva de riscos de segurança cibernética e de privacidade que podem ser identificados na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de *hackers*;
- Tratamento de dados em desconformidade com a LGPD;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em *link* malicioso ("*Phishing*");
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de *software* em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
- Vazamento de informações e dados pessoais durante tráfego de dados não criptografados.

5 Ações de prevenção e proteção

A M Square estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Todas as informações encontradas nos ambientes da M Square são tratadas como confidenciais e sigilosas, e as orientações de tratamento encontram-se na presente Política, no capítulo sobre a Política de Confidencialidade e Segurança da Informação e Comunicação com o Público no Manual de *Compliance*, e no capítulo sobre Código de Ética da Gestora, divulgados para todos os Colaboradores da Gestora, em especial os com acesso às informações e aos sistemas da Gestora, incluindo orientações que definem a maneira pela qual devem usar a tecnologia dentro da M Square.

5.1 Comunicações eletrônicas

Os Colaboradores devem observar que qualquer e-mail ou mensagem instantânea ("**MI**") que constitua um registro sobre qualquer atividade, transação ou negócio da Gestora é mantido pela M Square.

5.1.1 Mensagem Instantânea

A M Square reconhece que, em determinados casos, a MI pode ser uma fonte valiosa de informação, bem como um método eficiente de comunicação. A Gestora, portanto, permite aos Colaboradores usar o recurso de MI para comunicações relacionadas a suas atividades enquanto as MIs são enviadas e recebidas usando a plataforma designada pela Gestora para tais comunicações (Microsoft Teams). Os Colaboradores são proibidos de usar uma plataforma não designada para enviar e receber MIs relacionadas às atividades de prestação de serviços da M Square..

5.1.2 Política de Retenção de Comunicações Eletrônicas

A M Square implantou uma "**Política de Retenção de E-mail**" em que a Gestora tentará reter todos os e-mails e mensagens instantâneas ("MIs"). A Política de Retenção de E-mail da Gestora é composta por diversos fatores:

- O(A) Diretor(a) de *Compliance* é responsável pela supervisão da política;
- Os Colaboradores são proibidos de conduzir suas atividades relacionadas aos Serviços Prestados pela M Square por meio de qualquer rede de comunicação não pré-aprovada pela M Square, tais como e-mail externo, mensagem instantânea ou mensagem de texto não fornecido pela Gestora ao Colaborador ou por qualquer outro método que não possa ser capturado pelo sistema de retenção de e-mail.
- Todas as comunicações eletrônicas contempladas pelas exigências aplicáveis de manutenção de registro estão identificadas e preservadas da forma adequada;
- O descarte permanente de e-mails da rede da M Square deve ser conduzido de uma forma que proteja a confidencialidade, mediante prévia avaliação e aprovação do(a) Diretor(a) de *Compliance*; e
- Todos os Colaboradores no momentos do início do vínculo com a Gestora, são informados sobre a Política de Retenção de Comunicações Eletrônicas.

A M Square e o(a) Diretor de *Compliance* garantirá que seus *backups* estejam funcionando e que a Gestora possa disponibilizar e-mails, caso solicitado por um regulador.

5.1.3 Uso de Ativos

A utilização dos ativos da M Square, incluindo computadores, telefones, Internet, programas de *mensagem* instantânea, e-mails e demais aparelhos se destina a fins profissionais, e deve ser feita com cuidado.

Infraestrutura

Todos os computadores da M Square são criptografados e gerenciados pelo MDM (*Mobile Device Management*) do *Office 365,* e. o(a) detentor(a) dos acessos, poderá resetar o equipamento, com prévia autorização do(a) Diretor(a) de *Compliance* ou em casos de perda, furto ou de ataque cibernético, imediatamente pela equipe da área de TI com autonomia para executar o reset.

Os computadores da M Square são fornecidos para o exclusivo uso dos Colaboradores no desempenho de suas atividades profissionais, mediante assinatura de um Termo de Responsabilidade.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Documentos imprescindíveis para as atividades dos Colaboradores da Gestora deverão ser salvos no Sharepoint.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Os usuários não são administradores das máquinas, não tendo privilégios para acessar conteúdo no perfil de outro possível usuário logado.
- Os Colaboradores devem informar a(o) Diretor(a) de Compliance e/ou para a Área Administrativa e para equipe de TI, por meio formal, qualquer identificação de dispositivo estranho conectado ao seu computador.
- Os Colaboradores devem tempestivamente comunicar Área Administrativa e/ou a equipe de TI qualquer situação de perda, furto ou suspeita de ataque cibernetico ao seu computador e aos demais equipamentos ou dispositivos móveis que permitam acesso a e-mail e MIs corporativos.

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe de TI ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do(a) Diretor(a) de *Compliance*.
- Todas as contas deverão ter o *Two-factor authentication* - 2FA devidamente ativado.

5.1.4 Dispositivos Móveis

Considerando que deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores, a M Square permite o uso de seus equipamentos portáteis. Por "dispositivo móvel", entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Gestora, ou aprovado e permitido pelo(a) Diretor(a) de *Compliance*, como: *notebooks*, *smartphones* e *pen drives* (mediante prévia autorização/liberação).

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os Colaboradores que utilizem tais equipamentos.

Todo dispositivo móvel é gerenciado pelo MDM (*Mobile Device Management*) do *Office 365*, e, com isso, o(a) detentor(a) dos acessos poderá resetar o aparelho em padrão de fábrica, com prévia autorização do(a) Diretor(a) de *Compliance* ou em casos de perda, furto ou de ataque cibernético, imediatamente pela equipe da área de TI com autonomia para executar o reset.

O Colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na M Square, mesmo depois de terminado o vínculo contratual mantido com a Gestora.

Todo Colaborador deverá ter o *Two-factor authentication (2FA)* devidamente instalado na sua conta de e-mail e VPN.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes. O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Gestora e/ou a terceiros.

5.1.5 Datacenter

O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado com acompanhamento de um Colaborador autorizado. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer Colaborador responsável pela administração de liberação de acesso.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a autorização do(a) Diretor(a) de *Compliance*.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável.

No caso de desligamento de Colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de Colaboradores autorizados.

5.1.6 *Uso de e-mail*

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da M Square, inclusive que contenha fins políticos locais ou do país (propaganda política). O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente. Em nenhuma hipótese um Colaborador pode emitir uma opinião por e-mail em nome da M Square, salvo se expressamente autorizado para tanto pelo(a) Diretor(a) de *Compliance*.

Acrescentamos que é proibido aos Colaboradores o uso de e-mail da M Square para as seguintes atividades:

- Enviar mensagens (i) não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Gestora; (ii) pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar; (iii) que torne seu remetente e/ou a Gestora vulnerável a ações civis ou criminais; (iv) com informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação; (v) que inclua material protegido por direitos autorais sem a permissão do detentor dos direitos; (vi) que contenha Dados Pessoais de Investidores e Colaboradores, exceto quando autorizado por esta Política ou pelo(a) Diretor(a) de *Compliance*, nos termos desta Política;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Gestora estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Gestora; (ii) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; (iii) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, bem como que vise:

- obter acesso não autorizado a outro computador, servidor ou rede;
- interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- burlar qualquer sistema de segurança;
- vigiar secretamente ou assediar outro usuário;
- acessar informações confidenciais sem explícita autorização do proprietário;
- acessar indevidamente informações que possam causar prejuízos a qualquer pessoa.

As mensagens de e-mail deverão incluir assinatura com o seguinte formato: (i) nome do Colaborador, Nome da empresa, *Disclaimer*, Telefone(s) e Correio eletrônico, conforme especificado pela equipe de TI da Gestora.

5.1.7 *Uso da Internet*

Todas as regras atuais da M Square visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa com a Internet ofereça um grande potencial de benefícios, também propicia riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a Gestora reserva-se o direito de monitorar e registrar todos os acessos a ela, nos termos da legislação aplicável. Como mencionado, os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da Gestora, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/Internet, estejam em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

A visualização de conteúdos que contenham dado discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física) obsceno, pornográfico ou ofensivo é terminantemente proibida.

Programas licenciados e instalados nos computadores, principalmente via Internet (“downloads”), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do(a) Diretor(a) de *Compliance*.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado poderá excluído pela equipe de TI. Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Gestora para fazer o *download* ou distribuição de *software*

ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O *download* e a utilização de programas de jogos são proibidos.

Colaboradores com acesso à internet não poderão efetuar *upload* (subida) de qualquer *software* licenciado à M Square ou de dados de sua propriedade a Terceiros (conforme definido nesta Política) e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados. Os Colaboradores não poderão utilizar os recursos da Gestora para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores.

O acesso a *softwares peer-to-peer* (Kazà, BitTorrent e afins) não serão permitidos. Já os serviços de *streaming* (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos, conforme definido pelo(a) Diretor(a) de *Compliance*. Não é permitido acesso a sites de proxy.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Gestora cooperará ativamente com as autoridades competentes.

5.1.8 Identificação e uso de senhas

Observado o disposto na Política de Confidencialidade e Segurança da Informação, a senha e *login* para acesso aos dados contidos em todos os computadores corporativos, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todos os dispositivos de identificação utilizados na M Square, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Gestora e a legislação (cível e criminal).

É também proibido o compartilhamento de login para funções de administração de sistemas. A Área Administrativa da M Square é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários não possuem perfil de administrador. E as senhas deverão ter pelo menos 8 caracteres, sendo um deles, especial.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada pelos próximos 30 minutos (caso não seja desbloqueada manualmente pelo administrador). Para o desbloqueio é necessário que o usuário entre em contato com a equipe de TI. Caso o Colaborador esqueça sua senha, ele deverá requisitar formalmente a troca, para que a equipe de TI realize o cadastro de uma nova senha. Deverá ser estabelecido um processo para a renovação de senha. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Assim que algum usuário for demitido ou solicitar demissão, a Área Administrativa deverá imediatamente comunicar tal fato à equipe de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

5.1.9 Reprodução e *Descarte*

É terminantemente proibido aos Colaboradores fazer cópias ou imprimir arquivos usados, gerados ou disponíveis na rede da M Square e circular em ambientes externos a M Square com esses arquivos, uma vez que tais arquivos contêm informações consideradas confidenciais, conforme descrito no “Instrumento de Política Comercial” e “Compromisso de Responsabilidade e Confidencialidade” presentes no Anexo VIII e Anexo IX do Código de Ética, respectivamente.

A proibição acima não se aplica quando as cópias ou impressão de arquivos forem usadas para executar ou desenvolver negócios e interesses da M Square. Nestes casos, os Colaboradores em

posse e guarda da cópia ou do arquivo impresso contendo as informações confidenciais serão diretamente responsáveis por sua boa conservação, integridade e manutenção de sua confidencialidade.

O descarte de informações confidenciais em meio digital ou físico deve ser feito de forma a impossibilitar sua recuperação.

Em consonância com as normas acima, os Colaboradores são proibidos de utilizar *pen drives* ou qualquer website de compartilhamento de informações (e.g. Dropbox, Google Drive, etc.) discos ou quaisquer outras mídias que não exclusivamente para o desempenho de sua atividade na M Square, casos exepcionais pode ser aprovados pelo(a) diretor(a) de Compliance. Tais permissões devem ser revisadas anualmente e aprovadas pelo Comitê de Compliance.

Todas as informações que possibilitem a identificação de um Investidor da M Square devem permanecer em arquivos de acesso restrito, e somente poderão ser copiadas ou impressas para o atendimento dos interesses da M Square ou do próprio Investidor. Tal restrição não se aplica na eventualidade de cumprimento de ordem de autoridade judicial ou extrajudicial determinando a disponibilização de informações sobre eventual Investidor da M Square, cujo atendimento deverá ser previamente comunicado a(o) Diretor(a) de *Compliance*.

5.1.10 Conexão na Rede da M Square

É proibida a conexão de qualquer equipamento na rede da M Square sem a prévia autorização pelas Área Administrativa e pela equipe da área de TI..

5.1.11 *Controles e Registros de Atividades*

A Gestora implementou controles robustos de acesso utilizando duplo fator de autenticação em seu sistema de e-mail, VPNs e nos sistemas críticos da M Square (Controle de acesso lógico adequado aos ativos da organização).

5.2 Procedimentos de Proteção de Dados e de Segurança Cibernética de Terceiros Contratados

Os parceiros, fornecedores, prestadores de serviços externos da M Square ("Terceiros") também podem representar uma fonte significativa de riscos de proteção de privacidade de dados e de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço e, assim como as demais contratações de Terceiros, envolve determinados riscos que devem ser levados em conta pela Gestora, demandando certos cuidados proporcionais a esta identificação de ameaças.

5.2.1 Avaliação dos Terceiros contratados

Nesse sentido, a área de *Compliance* da Gestora deverá verificar o conteúdo mínimo de *Compliance* em segurança cibernética de Terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (*links*) com a Gestora, (iv) tratam dados pessoais relacionados às atividades da M Square ou (iv) qualquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de privacidade e de cibersegurança à Gestora, previamente à sua contratação, na forma do Anexo A desta Política.

Com base em tal verificação, o(a) Diretor(a) de *Compliance* avaliará a capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

5.2.2 Requisitos de segurança da informação nos contratos com Terceiros

A Gestora deverá incluir em contratos com Terceiros cláusulas de proteção de dados pessoais, requisitos de segurança da informação, bem como assegurar que os Terceiros contratados tenham políticas próprias de proteção de dados e de segurança cibernética e verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

Como forma de monitoramento o(a) Diretor(a) de Compliance solicitará esporadicamente aos Terceiros acesso as regras, procedimentos e controles internos bem como a Política de Privacidade e de Segurança da Informação adotados pela empresa.

6 Monitoramento e Testes Periódicos

Os mecanismos de supervisão para cada risco identificado no item 3 acima se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

A M Square investe em ferramentas robustas para monitoramento do ambiente, como também, em equipe especializada através da implementação do Network Operation Center ("NOC") e periodicamente realiza a atualização de seus ativos, a qual é registrada em um sistema pertinente, com a geração de relatórios mensais. O NOC monitora todos os *backups*, os quais são testados através de visualização dos dados salvaguardados.

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

- Implantar sistemas de monitoramento nos dispositivos corporativos, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Para os riscos associados a *Phishing*, conduzir treinamentos e campanhas periódicas, bem como testes de *Phishing*, ao menos anualmente;
- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela M Square, ao menos anualmente.

Periodicamente, a Gestora revisa o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de privacidade e cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Comitê de Risco e *Compliance* julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

7 Plano de Resposta a Incidentes

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Contingência e Recuperação de Desastre, anexo ao Manual de *Compliance* da Gestora ("Plano"), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores deverão imediatamente comunicar e reportar verbalmente quaisquer incidentes diretamente a(o) Diretor(a) de *Compliance* e/ou para a Área Administrativa e, em seguida, registrar o incidente por meio do canal de reporte de incidentes: E-mail: Compliance@msquare.com.br.

7.1 Procedimento em caso de incidente

Uma vez que o(a) Diretor(a) de *Compliance* tenha sido acionado devido a um potencial incidente, este deverá convocar o Comitê de Privacidade e Segurança Cibernética para:

Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

Incidente Caracterizado

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à CVM, ANBIMA, Agência Nacional de Proteção de Dados ("ANPD") ou outra autoridade competente, (ii) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor ou Colaborador que tenha sido afetado; e (iv) houve prejuízo para a Gestora, algum Veículo de Investimento ou Investidor específico. Além disso, o Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um acompanhamento, conforme o caso, em periodicidade a ser definida, com um sumário elaborado pelo(a) Diretor(a) de *Compliance* contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá se avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, tais como manifestação pública na mídia, com eventual contração de PR, enquanto que o Comitê de Investimentos verificará se todas as informações necessárias ao portfólio estão seguras e a área de gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados ao Comitê. Terceiros relevantes deverão ser mantidos atualizados.

Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao *full Compliance*, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado, como o sistema de gerenciamento, Compli.ly.

8 Reciclagem e revisão

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

Também realizará campanha de conscientização em privacidade e cibersegurança, com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger dados pessoais e outras informações como parte de suas responsabilidades por meio do Programa de Treinamento da Gestora.

O(A) Diretor(a) de *Compliance* realizará a revisão e atualização desta Política periodicamente, sempre que algum fato relevante ou evento motive sua revisão, conforme análise e decisão do(a) Diretor(a) de Compliance.

9 Termos e Definições

- Website – https://www.msquare.com/ e demais páginas deste domínio.

MODELO DE DILIGÊNCIA COM TERCEIROS DO GRUPO TÉCNICO DE CIBERSEGURANÇA DA ANBIMA

CONTEÚDO MÍNIMO DE *COMPLIANCE* EM SEGURANÇA CIBERNÉTICA A SER VERIFICADO

Compliance	Respostas
1. A empresa tem políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança? a. Se sim, é objeto de teste ou auditoria periódica? b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante?	
2. A empresa apresenta plano de resposta a incidentes de cibersegurança?	
3. A empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários?	
4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante?	
5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta.	
6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clientes e/ou reguladores (quando aplicável)?	
Favor disponibilizar os seguintes documentos: • Programa de segurança cibernética: se a organização segue políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica. • Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço.	