M. SAFRA & CO.

MANUAL DE COMPLIANCE E CÓDIGO DE ÉTICA

Este Manual de *Compliance* e Código de Ética ("Manual") tem por objetivo determinar as normas éticas e padrões de conduta básicos da M. Safra & Co. (nome fantasia de AMS Capital Ltda., a seguir denominada "Empresa"), que devem ser observados na condução de suas atividades e no relacionamento com clientes e agentes do mercado por todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a Empresa.

A Empresa deverá preparar e manter versões atualizadas deste Manual em seu website (*http://www.msafra.com.br/*), juntamente com os seguintes documentos: (i) Formulário de Referência, cujo conteúdo deve refletir o Anexo 15-II da ICVM 558; (ii) Política de Gestão de Risco; (iii) Diretrizes para Negociação e Investimentos; e (iv) Política de Rateio e Divisão de Ordens entre as carteiras de valores mobiliários.

Todo Colaborador, ao receber este Manual, e anualmente, firmará o Termo de Ciência das Normas Internas. Por esse documento, o Colaborador reconhece e confirma seu conhecimento e sua concordância com os termos deste Manual e demais políticas listadas no respectivo Termo e com as normas, princípios, conceitos e valores aqui contidos; comprometendo-se a zelar pela aplicação das normas de *compliance* e princípios contidos neste Manual. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Ciência das Normas Internas, reforçando o conhecimento e a concordância com os termos deste Manual.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da Empresa deverá ser levado para apreciação do Diretor de *Compliance* e Risco (conforme definido abaixo), de acordo com os procedimentos estabelecidos neste Manual. Competirá ao Diretor de *Compliance* e Risco (conforme definido abaixo) aplicar as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar o Diretor de *Compliance* e Risco sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Empresa, bem como zelar pela reputação da Empresa. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de *Compliance* e Risco, o Colaborador deverá informar diretamente os demais administradores da Empresa.

I. CÓDIGO DE ÉTICA

1. Objetivo

Os preceitos básicos que regem as atividades da Empresa e a atuação de seus Colaboradores são as seguintes:

Em sua atuação, a Empresa deverá sempre (i) exercer suas atividades com boa fé, transparência, diligência e lealdade em relação aos seus clientes, e (ii) desempenhar suas atribuições de modo a: (a) buscar atender aos objetivos de investimento de seus clientes, e (b) evitar práticas que possam ferir a relação mantida com seus clientes.

A Empresa zela pelo cumprimento fielmente do regulamento dos fundos de investimento sob sua gestão, os quais deverão incluir, no mínimo, os seguintes serviços a serem prestados: (i) política de investimentos a ser adotada, (ii) os riscos inerentes aos diversos tipos de operações com valores mobiliários nos mercados de bolsa, de balcão, nos mercados de liquidação futura e nas operações de empréstimo de ações que pretenda realizar com os recursos do cliente, e (iii) o conteúdo e a periodicidade das informações a serem prestadas aos clientes.

2. Relação com Meios de Comunicação

A Empresa vislumbra nos meios de comunicação um canal relevante de informação para os diversos segmentos da Empresa e está aberta a atender suas solicitações, sempre que isso for possível e não existirem obstáculos legais ou estratégicos, que serão explicitados aos jornalistas quando ocorrerem. O representante da Empresa perante qualquer meio de comunicação é, exclusivamente, seu Diretor Presidente, que poderá delegar essa função sempre que considerar adequado.

II. MANUAL DE COMPLIANCE

1. Responsabilidades e Obrigações

1.1. A coordenação direta das atividades relacionadas a este Manual é uma atribuição do diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos e da Instrução CVM 558 da Empresa (neste Manual e nas demais Políticas da Empresa, "Diretor de *Compliance* e Risco"), na qualidade de diretor estatutário da Empresa.

1.2. A Empresa conta, ainda, com o Comitê de *Compliance*, o qual é composto pelo Diretor Presidente, Diretor Responsável pela Administração de Carteiras de Valores Mobiliários, Diretor de *Compliance* e Risco e a Diretora Jurídica e tem como função principal a implementação e o monitoramento do cumprimento do Manual de *Compliance*, do Código de Ética e das demais Políticas da Empresa. As reuniões acontecem no mínimo anualmente e sempre que necessário e não há registro em ata das discussões e decisões tomadas. Quando necessária, a formalização ocorre por *e-mail*.

1.3. O Diretor de *Compliance* e Risco e o Comitê de *Compliance* exercem suas atividades de forma completamente independente e poderão exercer seus poderes e autoridade com relação a qualquer Colaborador.

2. Dúvidas ou ações contrárias aos princípios e normas do Manual

2.1. Em caso de dúvida em relação a quaisquer das matérias constantes deste Manual, também é imprescindível que se busque auxílio imediato junto ao Diretor de *Compliance* e Risco para obtenção de orientação mais adequada.

3. Acompanhamento das Políticas descritas neste Manual

3.1. Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual ou aplicáveis às atividades da Empresa que cheguem ao conhecimento do Diretor de *Compliance* e Risco, de acordo com os procedimentos estabelecidos neste Manual, o Diretor de *Compliance* e Risco utilizará os registros e sistemas disponíveis aos Colaboradores para verificar a conduta dos Colaboradores envolvidos.

3.2. Todo conteúdo que está na rede, bem como computadores e arquivos pessoais salvos, podem ser acessados caso o Diretor de *Compliance* e Risco ou o Comitê de *Compliance* julgue necessário. Da mesma forma, mensagens de correio eletrônico poderão ser gravadas e, quando necessário, interceptadas, sem que isto represente invasão da privacidade dos Colaboradores já que se tratam de ferramentas de trabalho disponibilizadas pela Empresa.

3.3. Adicionalmente, poderá ser realizado um monitoramento **anual**, a cargo do Diretor de *Compliance* e Risco, sobre o total, ou uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de *Compliance* e Risco, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas no presente Manual.

3.4. O Diretor de *Compliance* e Risco poderá utilizar as informações obtidas em tais sistemas para, após deliberação pelo Comitê de *Compliance*, eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos deste Manual. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

3.5. O Diretor de *Compliance* e Risco deverá ainda verificar periodicamente os níveis de controles internos e *compliance* junto a todas as áreas da Empresa, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos neste Manual, propondo a criação de novos controles e melhorias naqueles considerados deficientes e monitorando as respectivas correções.

4. Sanções (*Enforcement*)

4.1. A eventual aplicação de sanções decorrentes do descumprimento dos princípios estabelecidos neste Manual é de responsabilidade do Diretor de *Compliance* e Risco, conforme deliberação em Comitê de *Compliance*, garantido ao Colaborador, contudo, amplo direito de defesa.

4.2. Podem ser aplicadas, entre outras, penas de advertência, suspensão, desligamento, no caso de Colaboradores que sejam sócios da Empresa, ou demissão de seu cargo no caso de Colaboradores que sejam empregados da Empresa, sem prejuízos do direito da Empresa de pleitear indenização.

4.3. A Empresa não assume a responsabilidade por Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Cabe ao Diretor de *Compliance* e Risco aplicar as sanções que eventualmente venham a ser definidas pelo Comitê de *Compliance* em relação a quaisquer Colaboradores.

5. Confidencialidade

5.1. As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na Empresa, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas, de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras, incluindo informações de clientes da Empresa.

5.2. É vedado, ainda, aos Colaboradores divulgar, sob qualquer circunstância, a terceiros fora do âmbito das atividades da Empresa (exceto se estritamente necessário e

por obrigação da função exercida pelo funcionário ou por força de lei ou decisão judicial, caso em que deverá comunicar ao Comitê de *Compliance* imediatamente), quaisquer Informações Confidenciais, conforme abaixo definido.

5.3. Todos os Colaboradores são obrigados a assinar um termo de confidencialidade que é renovado **anualmente**.

5.4. Caso a Empresa venha a contratar terceiros para a prestação de serviços e estes venham a ter acesso a Informações Confidenciais, conforme abaixo definido, o contrato de prestação de serviços deverá prever cláusula de confidencialidade e, ainda, o estabelecimento de multa em caso de quebra de sigilo. Além disso, o funcionário do terceiro contratado que tiver acesso a Informações Confidenciais, conforme abaixo definido, deverá assinar pessoalmente um termo de confidencialidade se comprometendo a guardar o sigilo das referidas informações.

5.5. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Manual, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Empresa, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos, incluindo:

a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos fundos;
c) Operações estruturadas, demais operações e seus respectivos valores analisadas ou realizadas pelos fundos;
d) Relatórios, estudos, opiniões internas sobre ativos financeiros;
e) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
f) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Empresa e a seus sócios ou clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Empresa e que ainda não foi devidamente levado a público;
g) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos;
h) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
i) Outras informações obtidas junto a Colaboradores, *trainees*, estagiários ou jovens aprendizes da Empresa ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

5.6. *Insider Trading* significa a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

5.7. "Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Empresa, de Informação Confidencial que possa ser usada com benefício na compra ou venda de títulos ou valores mobiliários.

5.8. Qualquer Colaborador que possuir Informações Confidenciais nos termos acima deverá comunicar o Diretor de *Compliance* e Risco em até 48 (quarenta e oito) horas do momento no qual tomou conhecimento das informações, para que este tome as devidas providências para restringir, conforme o caso, a negociação com os títulos e valores mobiliários a que se referem as informações privilegiadas.

5.9. *Front-running* significa a prática que envolve aproveitar alguma informação privilegiada para realizar ou concluir uma operação antes de outros.

5.10. O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a Empresa, mas também após o seu término.

5.11. Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

5.12. **É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste Manual e na legislação aplicável.**

6. Potenciais Conflitos de Interesse

6.1. Conflitos de interesse são situações decorrentes do desempenho das funções de determinado Colaborador, nas quais os interesses pessoais de tal Colaborador possam ser divergentes ou conflitantes com os interesses da Empresa e/ou entre os interesses diferentes de dois ou mais de seus clientes, para quem a Empresa tem um dever para cada um ("Conflito de Interesses").

6.2. Caso a Empresa venha a exercer outras atividades no mercado, deverá informar seus clientes e incluir no regulamento dos fundos sob gestão informações sobre potenciais Conflitos de Interesse existentes entre tais atividades e a gestão dos recursos dos fundos.

6.3. Qualquer Conflito de Interesse deve ser sempre solucionado de forma a beneficiar o cliente.

7. Vantagens, Benefícios, Presentes e *Soft Dollar*

7.1. A Empresa tem por política transferir aos fundos geridos qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de gestora, salvo se for de outra maneira expressamente determinado pelo regulamento do fundo em questão. As operações de *soft dollar* somente ocorrerão se aprovadas pelo Comitê de Compliance e se em benefício dos fundos sob gestão, sendo que não haverá favorecimento da parte que oferecer esse tipo de serviço.

7.2. É vedado aos Colaboradores receber diretamente presentes de prestadores de serviços ou quaisquer terceiros que sejam oferecidos em decorrência das atividades da Empresa. No caso de recebimento de presentes, estes deverão ser entregues à diretoria que o sorteará entre todos os Colaboradores e diretores da Empresa.

7.3. Da mesma maneira, cursos viagens e afins somente poderão ser aceitos se aprovados pelo Comitê de *Compliance* e se a viagem for no interesse exclusivo da Empresa para melhor capacitação de seus profissionais.

8. Diretrizes para Negociação e Investimentos pelos Colaboradores

8.1. As Diretrizes para Negociação e Investimentos tem por objetivo reiterar a política e os parâmetros que devem reger as atividades dos Colaboradores em negociações de papéis e investimentos financeiros em geral. Tais Diretrizes foram elaboradas com o objetivo de reafirmar os princípios éticos do mais alto nível que sempre regeram as atividades da Empresa.

8.2. As Diretrizes para Negociação e Investimentos estão anexas a este Manual como Anexo I.

9. Política de Segurança da Informação e Segurança Cibernética

9.1. A Política de Segurança da Informação e Segurança Cibernética visa consolidar as regras aplicáveis ao uso dos equipamentos e de todos os recursos que envolvam tecnologia da informação, incluindo comunicação de dados e voz, pelos Colaboradores.

9.2. A Política de Segurança da Informação e Segurança Cibernética está anexa a este Manual como Anexo II. Regras adicionais e/ou mais específicas de segurança e de utilização dos recursos de tecnologia são divulgadas pelo Departamento de Tecnologia ou pelo Comitê de Tecnologia de acordo com a necessidade e estarão sempre disponíveis em locais de acesso comum na rede.

10. Segregação Física de Atividades

10.1. A Empresa desempenha atividades voltadas para a administração de carteiras de valores mobiliários, na categoria gestora de recursos, a qual é autorizada e exercida nos termos do inciso II do §1º do Art. 2º da Instrução CVM nº 558/15.

10.2. As atividades desenvolvidas pela Empresa são exaustivamente reguladas, especialmente pela Comissão de Valores Mobiliários ("CVM") e consistem exclusivamente na gestão de fundos de investimento, não havendo necessidade, portanto, de segregação de atividades. Contudo, caso a Empresa venha a desempenhar outra atividade, esta fará com que as instalações físicas da área responsável pela atividade de gestão de recursos de terceiros sejam fisicamente segregadas das demais áreas da mesma.

10.3. Os Colaboradores cuja atividade esteja diretamente relacionada com a administração de recursos terão linhas telefônicas especificas e monitoradas e acesso a diretórios de rede privativos e restritos, totalmente segregados dos demais Colaboradores da Empresa.

10.4. Considerando que a Empresa poderá contratar terceiros para a prestação de serviços de *back-office* e análise de valores mobiliários, a Empresa adota regras e procedimentos internos capazes de assegurar a completa segregação de funções, atividades e responsabilidades relacionadas com a gestão de fundos de investimento de que é gestora.

10.5. Caso a Empresa contrate os serviços mencionados acima, todos os Colaboradores que tiverem suas atividades profissionais relacionadas com a administração de carteiras de valores mobiliários serão alocados em local diverso dos demais prestadores de serviços, incluindo acesso exclusivo por meio de ponto eletrônico, utilização de instalações físicas totalmente independentes e segregadas, disponibilização de linhas telefônicas específicas e diretório de rede privativo e restrito, acessível somente mediante login e senha individuais.

11. Implementação do Presente Código

11.1. A conformidade com políticas internas é monitorada frequentemente. Os Colaboradores ratificam formalmente, **anualmente**, que conhecem e respeitam todas as regras de *compliance*, incluindo este Manual e as demais políticas da Empresa.

11.2. Em cumprimento ao artigo 16, VIII da Instrução CVM nº 558/2016, os Colaboradores deverão informar o Comitê de *Compliance* imediatamente quando da ocorrência ou indício de violação da legislação que incumbe à CVM fiscalizar. O Diretor de *Compliance* e Risco deverá informar a CVM sobre tal fato em até dez dias úteis da ocorrência ou identificação de tal fato.

12. Política de Treinamento

12.1. A Empresa possui um processo de treinamento inicial de todos seus Colaboradores, especialmente aqueles que tenham acesso a Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos princípios éticos, das leis e normas aplicáveis às suas atividades.

12.2. Assim que cada Colaborador é contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Empresa e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

12.3. Neste sentido, a Empresa adota um programa de reciclagem dos seus Colaboradores, que será executado, no mínimo, **anualmente** ou à medida que as regras e conceitos contidos neste Manual sejam atualizados, com o objetivo de fazer com que os Colaboradores estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

12.4. A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de *Compliance* e Risco e exige o comprometimento total dos Colaboradores quanto à sua assiduidade e dedicação.

12.5. Tanto o processo de treinamento inicial, quanto o programa de reciclagem deverão abordar as atividades da Empresa, seus princípios éticos e de conduta, as normas de *compliance*, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Manual (especialmente aquelas relativas à confidencialidade, segurança das informações e negociação pessoal), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades.

12.6. O Diretor de *Compliance* e Risco poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.

13. Lavagem de Dinheiro e Conheça seu Cliente (*Know Your Customer* ou "KYC")

Lavagem de Dinheiro

13.1. Seguindo o determinado pela Lei 9.613, de 03 de março de 1998 e de acordo com a Circular 3.461, de 24 de agosto de 2009 e Carta-Circular 3.542, de 12 de março de 2012, ambas editadas pelo Banco Central do Brasil, bem como a Instrução CVM nº 301, de 16 de abril de 1999, conforme alterada, e o Ofício-Circular nº 5/2015/SIN/CVM, a prevenção da utilização dos ativos e sistemas da Empresa para fins ilícitos, tais como crimes de "lavagem de dinheiro" e ocultação de bens e valores, é dever de todos os Colaboradores da Empresa.

13.2. A responsabilidade direta pelas questões relacionadas aos crimes de lavagem de dinheiro e ocultação de bens e valores será do Diretor de *Compliance* e Risco.

13.3. Qualquer suspeita de operações financeiras e não financeiras que possam envolver atividades relacionadas aos crimes de lavagem de dinheiro, ocultação de bens e valores, bem como incorporar ganhos de maneira ilícita, para a Empresa, clientes ou para o Colaborador, devem ser comunicadas imediatamente ao Diretor de *Compliance* e Risco.

13.4. A análise será feita caso a caso, ficando sujeitos os responsáveis às sanções previstas neste Manual, inclusive desligamento ou exclusão no caso de Colaboradores que sejam sócios da Empresa, ou demissão no caso de Colaboradores que sejam empregados da Empresa e ainda às consequências legais cabíveis.

13.5. Caberá ao Comitê de *Compliance* o monitoramento e a fiscalização do cumprimento, pelos Colaboradores, administradores e custodiantes dos fundos, da presente política de combate à "lavagem de dinheiro" da Empresa. Nesse sentido, tem a função de acessar e verificar periodicamente e no que for possível, as medidas de combate à lavagem de dinheiro adotadas pela Empresa e pelos administradores e custodiantes dos fundos que são ou venham a ser geridos pela Empresa, sugerindo inclusive a adoção de novos procedimentos ou alterações nos controles já existentes.

13.6. A negociação de ativos e valores mobiliários financeiros e valores mobiliários para os fundos deve, assim como o passivo, ser igualmente objeto de análise, avaliação e monitoramento para fins de prevenção e combate à lavagem de dinheiro.

13.7. O Diretor de *Compliance* e Risco, ao receber a comunicação, analisará a informação junto ao Comitê de *Compliance*, e conduzirá o caso às autoridades competentes, se julgar pertinente. A análise será feita caso a caso, mediante avaliação dos instrumentos utilizados, a forma de realização, as partes e valores envolvidos, a capacidade financeira e a atividade econômica do cliente e qualquer indicativo de irregularidade ou ilegalidade envolvendo o cliente ou suas operações.

13.8. O Diretor de *Compliance* e Risco emitirá relatório anual listando as operações identificadas como suspeitas, e as operações ou propostas de operações que, na forma da legislação vigente, caracterizam indício de lavagem de dinheiro, e foram devidamente comunicadas às autoridades competentes. Os processos de registro, análise e comunicação, às autoridades competentes, de operações financeiras que revelam indício de lavagem de dinheiro são realizados de forma sigilosa, inclusive em relação aos clientes.

13.9. Nas operações ativas (investimentos), o "cliente" deve ser entendido como a contraparte da operação, sendo a Empresa responsável pelo seu cadastro e monitoramento, se for o caso.

13.10. Neste contexto, para os fundos de investimento, dentro do princípio da razoabilidade e agindo com bom senso, a Empresa deverá se utilizar das práticas descritas neste Manual, conforme estabelecido no Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro divulgado pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA").

13.11. Já com relação aos clientes e investidores dos produtos oferecidos pela Empresa, a análise, avaliação e monitoramento para fins de prevenção e combate à lavagem de dinheiro será realizada com base nas regras de KYC descritas abaixo.

Processo de Identificação de Contrapartes (Cadastro)

13.12. A Empresa deve estabelecer processo de identificação de contraparte (cliente) adequado às características e especificidades dos negócios. Tal processo visa a prevenir que a contraparte utilize os fundos de investimento geridos para atividades ilegais ou impróprias.

13.13. Os ativos e valores mobiliários elencados a seguir, em função de sua contraparte e do mercado nos quais são negociados, já passaram por processo de verificação, o que, em princípio, acabaria por eximir a Empresa de diligência adicional em relação ao controle da contraparte, a saber: (a) ofertas públicas iniciais e secundárias de valores mobiliários, registradas de acordo com as normas emitidas pela CVM; (b) ofertas públicas de esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM; (c) 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; (d) ativos e valores mobiliários cuja contraparte seja instituição financeira ou equiparada; e (e) ativos e valores mobiliários de mesma natureza econômica daqueles acima listados, quando negociados no exterior, desde que (i) 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 (ii) 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.

13.14. No entanto, a Empresa sempre diligenciará no processo de identificação da contraparte, caso seja possível tal diligência em razão das circunstâncias e características do ativo a ser investido.

Monitoramento: Controle do Preço dos Ativos e Valores Mobiliários Negociados

13.15. A Empresa deve adotar procedimentos com vistas a controlar e monitorar a faixa de preços dos ativos e valores mobiliários negociados para os fundos, de modo que

eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas e, se for o caso, comunicados aos órgãos competentes.

Comunicação ao COAF

13.16. As situações listadas abaixo podem configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613, ou podem com eles relacionar-se, devendo ser analisadas com especial atenção e, se e quando consideradas suspeitas por Colaboradores, nos termos do art. 6º e 7º da ICVM 301/99, comunicadas ao Conselho de Controle de Atividades Financeiras - COAF:

(a) Realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo, que apresentem atipicidade em relação à atividade econômica do cliente ou incompatibilidade com a sua capacidade econômico-financeira.

(b) Resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral, oferecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação.

(c) Apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente.

(d) Solicitação de não observância ou atuação no sentido de induzir Colaboradores da instituição a não seguirem os procedimentos regulamentares ou formais para a realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo.

(e) Quaisquer operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo envolvendo pessoas relacionadas a atividades terroristas listadas pelo Conselho de Segurança das Nações Unidas.

(f) Realização de operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários, qualquer que seja o valor da aplicação, por pessoas que reconhecidamente tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento.

(g) Quaisquer operações ou conjunto de operações de compra ou venda de títulos e valores mobiliários com indícios de financiamento do terrorismo.

(h) Operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários fora dos padrões praticados no mercado.

(i) Realização de operações que resultem em elevados ganhos para os agentes intermediários, em desproporção com a natureza dos serviços efetivamente prestados; investimentos significativos em produtos de baixa rentabilidade e liquidez,

considerando a natureza do fundo ou o perfil do cliente/mandato da carteira administrada.

(j) Operações nas quais haja deterioração do ativo sem fundamento econômico que a justifique.

13.17. Os registros das conclusões de suas análises acerca de operações ou propostas que fundamentaram a decisão de efetuar, ou não, as comunicações de que trata o parágrafo acima devem ser mantidas pelo prazo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, em caso de processo administrativo.

Conheça seu Cliente (KYC)

13.18. O processo de KYC consiste na análise e identificação do investidor de modo a identificar e conhecer a origem e constituição de seu patrimônio e de seus recursos financeiros, com o objetivo de inibir a entrada ou manutenção de clientes na instituição que tenham ligação com a lavagem de dinheiro ou outras atividades ilícitas.

13.19. A Empresa contará com esforços dos administradores e custodiantes dos fundos que são ou venham a ser por ela geridos para (i) realizar a identificação de clientes novos ou já existentes, inclusive previamente à efetiva realização dos investimentos; e (ii) prevenir, detectar e reportar quaisquer operações suspeitas. Nesse sentido, o Diretor de *Compliance* e Risco poderá acompanhar as atividades dos administradores e custodiantes, de modo a verificar se os procedimentos e regras de identificação e atualização de dados cadastrais de investidores, bem como controles para detecção de operações suspeitas foram efetivamente implementados e estão sendo diligentemente cumpridos, de acordo com a Instrução CVM nº 301/99, conforme alterada, e o Ofício-Circular nº 5/2015/SIN/CVM.

13.20. Os Colaboradores da Empresa, nas atividades desempenhadas pela Empresa, ou os administradores e custodiantes dos fundos (sob a supervisão do Diretor de *Compliance* e Risco) deverão estabelecer uma análise independente e assegurar um processo reforçado de *due diligence* com relação às Pessoas Politicamente Expostas ("PEP"), definidas como pessoas que exerceram altos cargos de natureza política ou pública, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

13.21. Independentemente do processo especial de KYC aplicável a estas categorias de Clientes, a aceitação de PEP como cliente da Empresa nos serviços por ela prestados depende sempre da autorização dos administradores da Empresa.

14. Política de Anticorrupção

14.1. A Empresa está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção").

14.2. Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Empresa e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

14.3. Quaisquer indícios ou suspeitas de violação desta Política de Anticorrupção e das Normas de Anticorrupção, seja pelos Colaboradores ou pelos prestadores de serviços da Empresa, deverão ser levados imediatamente ao conhecimento do Diretor de *Compliance* e Risco, o qual investigará o caso e o levará para discussão no Comitê de *Compliance.*

Abrangência das Normas de Anticorrupção

14.4. Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

14.5. Considera-se agente público e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

14.6. Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

14.7. As mesmas exigências e restrições também se aplicam aos familiares de Colaboradores públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

14.8. Representantes de fundos de pensão públicos, cartorários e assessores de colaboradores públicos também devem ser considerados “agentes públicos” para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

14.9. Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

I prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

III comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
d) fraudar licitação pública ou contrato dela decorrente;
e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

V dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

14.10. É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público.

14.11. Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público.

14.12. Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontrem previsão legal ou regulamentar.

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

15. Política de Certificação

Introdução

15.1. A Empresa aderiu e está sujeita às disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código de Certificação"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

Atividades Elegíveis e Critérios de Identificação

15.2. Tendo em vista a atuação exclusiva da Empresa como gestora de recursos de terceiros, a Empresa identificou, segundo o Código de Certificação, que a Certificação de Gestores ANBIMA ("CGA") é a certificação descrita no Código de Certificação pertinente às suas atividades, aplicável aos profissionais com alçada/poder discricionário de investimento, nos termos do Art. 28 do Código de Certificação.

15.3. Nesse sentido, a Empresa definiu que qualquer Colaborador com poder para ordenar a compra ou venda de posições sem aprovação prévia do Diretor Responsável pela Administração de Carteira de Valores Mobiliários é elegível à CGA.

15.4. Em complemento, a Empresa destaca que a CGA é pessoal, intransferível e válida por tempo indeterminado, desde que o Colaborador esteja exercendo a atividade de gestão de recursos na Empresa e a CGA não esteja vencida a partir do vínculo da Empresa, não existindo, conforme disposto no Código de Certificação, procedimentos de atualização obrigatórios.

Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA

15.5. Antes da contratação ou admissão de qualquer Colaborador, o Diretor de *Compliance* e Risco deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação.

15.6. Conforme acima exposto, a CGA é, atualmente, a certificação ANBIMA aplicável às atividades da Empresa, de forma que o Diretor Responsável pela Administração de Carteira de Valores Mobiliários deverá esclarecer ao Diretor de *Compliance* e Risco se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de investimento.

15.7. Caso seja identificada a necessidade de certificação, o Diretor de *Compliance* e Risco deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

15.8. O Diretor de *Compliance* e Risco também deverá checar se Colaboradores que estejam se desligando da Empresa estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Empresa.

15.9. Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer até o último dia útil do mês subsequente à data do evento que deu causa a atualização, nos termos do Art. 12, §1º, I do Código de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de *Compliance* e Risco, conforme disposto abaixo.

Rotinas de Verificação

15.10. Mensalmente, o Diretor de *Compliance* e Risco deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados.

15.11. Ainda, sem prejuízo de o Diretor de *Compliance* e Risco contatar, mensalmente, o Diretor Responsável pela Administração de Carteira de Valores Mobiliários para verificar se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso, o Diretor Responsável pela Administração de Carteira de Valores Mobiliários deve informar imediatamente o Diretor de *Compliance* e Risco sempre que houver algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos.

15.12. Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Art. 17 do Código de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Empresa.

15.13. Ademais, no curso das atividades de *compliance* e fiscalização desempenhadas pelo Diretor de *Compliance* e Risco, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor Responsável pela Administração de Carteira de Valores Mobiliários ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente, o Diretor de *Compliance* e Risco poderá declarar de imediato o afastamento do Colaborador, sendo que o Comitê de *Compliance* deverá se reunir extraordinariamente para apuração das potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

15.14. Sem prejuízo do disposto acima, anualmente deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação,

sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de *compliance.*

15.15. Por fim, serão objeto do treinamento anual de *compliance* assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Empresa, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos, reforçando que somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Empresa, devendo os demais buscar aprovação junto ao Diretor Responsável pela Administração de Carteira de Valores Mobiliários ; e (iii) treinamento direcionado aos Colaboradores da área de *Compliance*, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

Processo de Afastamento

15.16. Todos os profissionais não certificados ou em processo de certificação, para os quais a certificação seja exigível, nos termos previstos neste Manual, serão, nos termos do art. 9º, §1ª, inciso V do Código de Certificação, imediatamente afastados das atividades de gestão de recursos de terceiros até que se certifiquem pela CGA.

15.17. Não obstante a cláusula acima, caso o profissional tenha sido indicado por meio de Termo de Adequação para adesão ao Código de Certificação, deverá obter no decorrer dos próximos dois exames da CGA após a celebração do Termo de Adequação, aprovação em ao menos um módulo do exame e devem atingir o estado de certificados pela CGA em até um ano a partir da celebração do Termo de Adequação.

15.18. Aos profissionais já certificados, caso deixem de ser Colaboradores da Empresa, deverão assinar documentação prevista no "Anexo III", denominado "Termo de Afastamento", comprovando o afastamento da Empresa, bem como os profissionais em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

Declaro que li, concordo, e me obrigo a observar o Código de Ética e Manual de *Compliance* da M. Safra & Co., bem como seus anexos:

Colaborador:

_____

Nome:
Data:

ANEXO I

DIRETRIZES PARA NEGOCIAÇÃO E INVESTIMENTOS

M. SAFRA & CO.

DIRETRIZES PARA NEGOCIAÇÃO E INVESTIMENTOS

I. INTRODUÇÃO

1.1. As Diretrizes para Negociação e Investimentos ("Diretrizes") têm por objetivo reiterar a política e os parâmetros que devem reger as atividades dos seus sócios, diretores e funcionários ("Colaboradores") da M. Safra & Co. (nome fantasia de AMS Capital Ltda., a seguir denominada "Empresa"), como instituição, em negociações de papéis e investimentos financeiros em geral. Estas Diretrizes foram elaboradas com o objetivo de reafirmar os princípios éticos do mais alto nível que sempre regeram esta instituição, além de preservar a Empresa e os Colaboradores de eventuais questionamentos de autoridades governamentais e/ou terceiros.

1.2. As Diretrizes orientam, mas não esgotam, os princípios éticos e legais aplicáveis aos investimentos efetuados pela Empresa e pelos Colaboradores, além de estabelecer procedimentos a serem observados pelos Colaboradores em operações em mercado de capitais e operações financeiras em geral ("Operações").

1.3. A Empresa, em conjunto com outras entidades, além de participar da gestão de fundos, também presta serviços de consultoria, administra e gere recursos de terceiros. Para fins desta política, as Operações relacionadas a essas atividades serão referidas simplesmente como "Investimentos".

1.3.1. Os Colaboradores realizam Operações com seus próprios recursos, os quais serão referidos neste documento como "Investimentos do Colaborador". Por "Investimentos do Colaborador" deve-se entender não só os investimentos efetuados em nome ou com recursos do Colaborador, mas também qualquer outro investimento no qual o Colaborador possa ter participação ou oportunidade de, direta ou indiretamente, auferir qualquer vantagem ou benefício (pecuniário ou não), inclusive, mas não se limitando a: (a) investimentos efetuados por seus parentes de primeiro grau, cônjuge ou companheiro, (b) qualquer pessoa a quem influencie ou seja por ela influenciado, (c) qualquer entidade da qual o Colaborador seja um beneficiário, (d) pessoas jurídicas com a qual o Colaborador tenha alguma ligação, (e) fundos dos quais participe, direta ou indiretamente, e (f) sociedades com as quais o Colaborador tenha celebrado algum tipo de acordo, entendimento ou relação.

1.4. É fundamental a leitura e o entendimento destas Diretrizes pelo Colaborador a fim de (a) preservar a linha de conduta ética da Empresa e do Colaborador, e (b) evitar que os Investimentos e os Investimentos do Colaborador possam resultar no descumprimento de leis e regulamentação aplicáveis às Operações a serem realizadas pelo Colaborador.

1.5. Ao ler e concordar com a sua assinatura no final deste documento, o Colaborador se declara ciente da destas Diretrizes devendo cumpri-las e observar os procedimentos nela estabelecidos.

1.6. Se o Colaborador pretender realizar qualquer Operação ou adotar qualquer conduta, mas tenha dúvida se tal Operação ou conduta possa ser equiparada a uma das práticas vedadas por estas Diretrizes, o Colaborador deverá, previamente, consultar o Comitê de *Compliance* da Empresa ("Comitê de *Compliance*"). Além disso, caso o Colaborador tenha qualquer dúvida ou sugestão referente a estas Diretrizes, deverá consultar o Comitê de *Compliance* para solucionar tal dúvida ou encaminhar a sugestão. Qualquer comunicação a ser efetuada ao Comitê de *Compliance* deve ser encaminhada, por mensagem eletrônica, para o endereço compliance@msafra.com.br, ao qual todos os membros do Comitê de *Compliance* têm acesso.

II. PRINCÍPIOS A SEREM OBSERVADOS PELOS COLABORADORES

2.1. Cabe ao Colaborador observar e respeitar as leis e regulamentos aplicáveis não só aos Investimentos que realiza, como também aos Investimentos do Colaborador. Tais leis e regulamentos têm publicidade e, conforme a legislação vigente, não podem deixar de ser observados mesmo por alegado desconhecimento do Colaborador.

2.1.2 Estas Diretrizes não constituem um guia exaustivo nem pretendem ser um resumo da legislação aplicável às Operações. Trata-se apenas de uma mera descrição geral dos princípios éticos básicos que devem reger os Investimentos e Investimentos do Colaborador, mediante a fixação de normas que têm a finalidade de evitar a realização de Operação que possa resultar, mesmo que involuntariamente, em (a) manipulação do mercado, (b) conflito de interesses, ou (c) utilização de informações privilegiadas, tanto pelo Colaborador ou que, por ter sido realizada pelo Colaborador possa, de alguma forma ser atribuída à Empresa ou qualquer de suas coligadas ou controladas.

2.1.3. As práticas descritas abaixo são expressamente vedadas aos Colaboradores, seja nos Investimentos ou nos Investimentos do Colaborador.

Manipulação do Mercado

2.2. A lei define manipulação do mercado como "realizar operações simuladas ou executar outras manobras fraudulentas destinadas a elevar, manter ou baixar a cotação, o preço ou o volume negociado de um valor mobiliário, com o fim de obter vantagem indevida ou lucro, para si ou para outrem, ou causar dano a terceiros" [1].

2.2.1. Inclui-se nessa prática o seguinte[2]:

[1] Artigo 27-C da Lei 6.385 de 7 de dezembro de 1976, conforme alterada.
[2] Instrução CVM nº8 de 8 de outubro de 1979.

(a) a criação de condições artificiais de demanda, oferta ou preço de valores mobiliários, que são criadas em decorrência de negociações pelas quais seus participantes ou intermediários, por ação ou omissão dolosa provocarem, direta ou indiretamente, alterações no fluxo de ordens de compra ou venda de valores mobiliários;

(b) a manipulação de preços no mercado de valores mobiliários, que é a utilização de qualquer processo ou artifício destinado, direta ou indiretamente, a elevar, manter ou baixar a cotação de um valor mobiliário, induzindo, terceiros à sua compra e venda; e/ou

(c) quaisquer operações fraudulentas no mercado de valores mobiliários, como por exemplo, as que utilizem ardil ou artifício destinado a induzir ou manter terceiros em erro, com a finalidade de obter vantagem ilícita de natureza patrimonial para as partes na operação, para o intermediário ou para terceiros.

Conflito de Interesses

2.3. Ocorre conflito de interesses quando o Colaborador se envolver, de algum modo, em alguma Operação que possa resultar em vantagem ou benefício (pecuniário ou não) ao Colaborador, seja por meio de manipulação do mercado ou influência nos Investimentos.

2.3.1. Para evitar tal situação, o Colaborador ao (i) recomendar ou realizar Investimentos, (ii) comentar notícias, fatos, resultados financeiros, dados econômicos, ou (iii) emitir opiniões relacionadas a macro ou micro economia ou quaisquer outros assuntos que possam, de alguma maneira, influenciar a decisão de Investimento da Empresa e dos demais Colaboradores e se tal recomendação, comentário, ou opinião puder, direta ou indiretamente, ter qualquer influência nos Investimentos do Colaborador ou na sua carteira de Investimentos, o Colaborador deverá informar tal fato aos destinatários de tal recomendação, comentário ou opinião.

2.3.2. A título de mera ilustração, são mencionados abaixo exemplos típicos de Operações que resultam em claro conflito de interesses e que, portanto, são vedados ao Colaborador:

(a) *Front Running*: é a realização de Investimentos do Colaborador em papéis dos quais o Colaborador tem conhecimento dos Investimentos, incluindo os respectivos planos de negociação e posição da Empresa e suas coligadas; e

(b) *Scalping*: é a realização de Investimento do Colaborador e posterior recomendação de Investimento com o fim de afetar o valor do papel objeto do Investimento do Colaborador;

2.3.3. Além das vedações acima, caso o Colaborador venha a ter conhecimento, formal ou informalmente, de alguma estratégia de mudança de posição dos Investimentos ou realização de novos Investimentos em papéis, os quais o Colaborador carregue em sua carteira (por meio de um Investimento do Colaborador), o Colaborador deverá, imediatamente, informar tal fato, por escrito, ao Comitê de *Compliance*.

2.3.4. Em casos de potencial conflito de interesse, a respectiva solução será sempre em favor dos clientes da Empresa.

Operações com Informações Privilegiadas (*Insider Trading)*

2.4. A lei define informação privilegiada como o ato de utilizar informação relevante, de que tenha conhecimento, ainda não divulgada ao mercado, que seja capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiros, de valores mobiliários ("Informação Privilegiada")[3].

2.4.1. São também consideradas "Informações Privilegiadas", dentre outras, aquelas que possam, de modo ponderável, influenciar na (a) cotação dos valores mobiliários de emissão de companhia aberta ou a eles referenciados, (b) decisão dos investidores de comprar, vender ou manter aqueles valores mobiliários, e (c) decisão dos investidores de exercer quaisquer direitos inerentes à condição de titular de valores mobiliários emitidos por certa companhia ou a eles referenciados.

2.4.2. São exemplos de informações de determinada sociedade que, se obtidas pelo Colaborador anteriormente ao conhecimento do mercado, são consideradas Informações Privilegiadas, as seguintes:

(a) assinatura de carta de intenções, memorando de entendimentos, ou de compromisso, acordo ou contrato de transferência do controle acionário da companhia, ainda que sob condição suspensiva ou resolutiva;

(b) mudança no controle da companhia, inclusive por meio de celebração, alteração ou rescisão de acordo de acionistas;

(c) celebração, alteração ou rescisão de acordo de acionistas em que a companhia seja parte ou interveniente, ou que tenha sido averbado no livro próprio da companhia;

(d) ingresso ou saída de sócio que mantenha, com a companhia, contrato ou colaboração operacional, financeira, tecnológica ou administrativa;

(e) autorização para negociação dos valores mobiliários de emissão da companhia em qualquer mercado, nacional ou estrangeiro;

(f) decisão de promover o cancelamento de registro da companhia aberta;

(g) incorporação, fusão ou cisão envolvendo a companhia ou empresas ligadas;

[3] Artigo 27-D da Lei 6.385 de 7 de dezembro de 1976, conforme alterada.

(f) transformação ou dissolução da companhia;

(g) mudança na composição do patrimônio da companhia;

(h) mudança de critérios contábeis;

(i) renegociação de dívidas;

(j) aprovação de plano de outorga de opção de compra de ações;

(k) alteração nos direitos e vantagens dos valores mobiliários emitidos pela companhia;

(l) desdobramento ou grupamento de ações ou atribuição de bonificação;

(m) aquisição de ações da companhia para permanência em tesouraria ou cancelamento, e alienação de ações assim adquiridas;

(n) lucro ou prejuízo da companhia e a atribuição de proventos em dinheiro;

(o) celebração ou extinção de contrato, ou o insucesso na sua realização, quando a expectativa de concretização for de conhecimento público;

(p) aprovação, alteração ou desistência de projeto ou atraso em sua implantação;

(q) início, retomada ou paralisação da fabricação ou comercialização de produto ou da prestação de serviço;

(r) descoberta, mudança ou desenvolvimento de tecnologia, de direitos ou de recursos da companhia;

(s) modificação de projeções divulgadas pela companhia; ou

(t) requerimento de recuperação judicial ou extrajudicial, confissão de falência ou propositura de ação judicial que possa vir a afetar a situação econômico-financeira da companhia.

2.4.3. É vedado ao Colaborador realizar qualquer Investimento ou Investimento do Colaborador, ou mesmo recomendar qualquer Investimento, em posse de qualquer Informação Privilegiada. É proibida também a divulgação de tal informação internamente e a terceiros. Caso o Colaborador tenha conhecimento de alguma informação privilegiada, deverá imediatamente relatar o fato ao Comitê de *Compliance*, o qual deverá decidir quais as providências a serem tomadas, a fim de evitar que qualquer Operação seja realizada de posse de tal informação.

Lista de Papéis Restritos

2.5. A Empresa manterá uma lista de papéis e companhias que não poderão ser objeto de Investimento ou Investimento do Colaborador (a "Lista de Papéis Restritos"), a qual está disponível na pasta "T:\Compliance\Lista de Papéis Restritos". Além da rigorosa observância dos procedimentos e restrições aqui mencionadas, o Colaborador

deverá abster-se de efetuar qualquer Investimento do Colaborador nos papéis e companhias relacionados na Lista de Papéis Restritos (incluindo, mas não se limitando, a ações, opções, bônus de subscrição ou qualquer outro valor mobiliário).

2.6. Os Colaboradores são vedados de (i) realizar operações/negociar com pessoas - ou valores mobiliários emitidos por países/jurisdições - que façam parte de listas de sanções financeiras, ou seja, que tenham sofrido medidas restritivas implementadas por organizações internacionais ou por países (a título individual) aplicáveis a jurisdições, pessoas ou entidades com o propósito de combater o terrorismo e manter ou restaurar a paz e a segurança internacional, e (ii) manter qualquer tipo de relacionamento com entidades conhecidas como *shell banks*, ou seja, instituições financeiras constituídas em jurisdições nas quais não tenha presença física e que não sejam afiliadas a grupos financeiros regulados.

2.7. É proibida a realização de qualquer Operação, seja qual for sua forma ou estrutura, que possa, de alguma maneira, ter objetivo ou resultado semelhante a qualquer uma das práticas mencionadas acima.

III. REGRAS PARA INVESTIMENTOS DO COLABORADOR

3.1. Além das regras mencionadas no Capítulo II, que se aplica a todo e qualquer Investimento do Colaborador, a realização de Investimentos do Colaborador estará sujeita às regras deste capítulo.

Operações Permitidas ao Colaborador

3.2. O Colaborador poderá realizar qualquer Investimento do Colaborador em papéis que tenham as seguintes características:

(a) títulos de renda fixa do governo federal;

(b) títulos públicos de emissão do governo federal;

(c) caderneta de poupança;

(d) fundos DI;

(e) fundos abertos com patrimônio superior a R$100.000.000,00 (cem milhões de reais);

(f) CDB de bancos de primeira linha;

(g) fundos referenciados;

(h) títulos de capitalização;

(i) debêntures não conversíveis de emissão pública; e/ou

(j) ações que:

(i) isoladamente ou no total da posição da carteira do próprio Colaborador, não ultrapasse R$ 500.000,00 (quinhentos mil reais);

(ii) não seja um papel ou de emissão de companhia que conste da Lista de Papéis Restritos;

(iii) em caso de aquisição, (1) a ação seja mantida por pelo menos 30 (trinta) dias na carteira do Colaborador e (2) o Colaborador não tenha alienado papéis da mesma emissora nos 30 (trinta) dias anteriores; e

(iv) em caso de alienação, o Colaborador não tenha adquirido papéis da mesma emissora nos 30 (trinta) dias anteriores.

Operações Sujeitas a Aprovação Prévia

3.3. Qualquer Investimento do Colaborador que não se enquadre em uma das Operações listadas no item 3.2 acima, estará sujeita à aprovação prévia de um membro do Comitê de *Compliance*, nos termos abaixo.

3.3.1. Sempre que for realizar um Investimento do Colaborador, o Colaborador deverá proceder da seguinte maneira:

(a) antes de realizar o Investimento do Colaborador, o Colaborador deverá preencher o formulário de pedido de aprovação, que está disponível na pasta "T:\Compliance\Formulário de Pedido de Aprovação para Investimento do Colaborador";

(b) o formulário deverá ser imediatamente encaminhado ao Comitê de *Compliance* (por mensagem eletrônica, no endereço compliance@msafra.com.br), que tem 24 (vinte e quatro) horas ou um dia útil (o que for mais longo) para autorizar ou não a Operação;

(c) caso o Colaborador não receba a manifestação por e-mail de um dos membros do Comitê de *Compliance* sobre a aprovação ou desaprovação da Operação no prazo mencionado no item (b) acima, a Operação pretendida deve ser considerada aprovada e o Colaborador poderá efetuá-la;

(d) embora o pedido de autorização não obrigue o Colaborador a efetuar a Operação, (i) o pedido deve ser efetuado apenas para Operações que o Colaborador pretenda efetivamente realizar, (ii) a Operação deverá ser efetuada em até 24 (vinte e quatro) horas ou um dia útil (o que for mais longo) do recebimento da aprovação, e partir do final deste prazo a autorização será considerada automaticamente cancelada e uma nova autorização deverá ser solicitada caso o Colaborador ainda pretenda realizar a Operação, e (iii) o Colaborador deverá manter sigilo sobre o pedido de autorização e sua respectiva aprovação ou desaprovação; e

(e) desaprovada a Operação, o Colaborador não poderá efetuá-la.

3.3.2. Ao receber o pedido de autorização para a realização de um Investimento do Colaborador, o Comitê de *Compliance* cumprirá procedimentos internos de verificação de checagem de conflito a fim de evitar a exposição do Colaborador e/ou da Empresa e suas coligadas e controladas a risco de imagem e situação de inobservância desta política ou da lei e regulamentação aplicável.

3.3.3. A aprovação ou vedação à Operação pretendida não será acompanhada de justificativa, uma vez que, ao tomar tal decisão e seguir os procedimentos internos de checagem de conflitos, o Comitê de *Compliance* tem acesso a informações privilegiadas tais como planos de investimentos e informações estratégicas da Empresa e suas coligadas ou controladas.

Condutas Incompatíveis

3.4. Por entender que os Investimentos do Colaborador realizados com as características abaixo listadas prejudicam o desempenho e a dedicação do Colaborador no cumprimento de suas funções, a Empresa desencoraja o Colaborador a adotar as seguintes práticas:

(a) alavancar investimentos em mais de 100% (cem por cento) do seu patrimônio;

(b) operar com corretoras que não sejam de primeira linha e/ou não tenham reputação ilibada no mercado;

(c) realizar Operações a descoberto em geral; e

(d) realizar Operações de curto prazo, as quais são vedadas pela presente política;

Fornecimento de Informações

3.5. A fim de fiscalizar o cumprimento desta política, o Diretor de *Compliance* e Risco e o Comitê de *Compliance*, conforme o caso, poderão, a qualquer tempo, solicitar ao Colaborador informações sobre os Investimentos do Colaborador.

IV. CONFIDENCIALIDADE

4.1. É vedado ainda ao Colaborador divulgar internamente, e sob qualquer circunstância a terceiros (exceto por força de lei ou decisão judicial, caso em que deverá comunicar ao Comitê de *Compliance* imediatamente), as posições, operações ou plano de operações da carteira de Investimentos sob sua responsabilidade. Tais informações poderão apenas ser reveladas se estritamente necessário e por obrigação da função exercida pelo Colaborador.

Vigente a partir de janeiro de 2019. **Atualizada em agosto de 2020.**

Declaro que li, concordo, e me obrigo a observar as Diretrizes para Negociação e Investimentos da M. Safra & Co.:

Colaborador:

_____

Nome:
Data:

ANEXO II

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

M. SAFRA & CO.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

I. INTRODUÇÃO

1.1. Esta Política de Segurança da Informação e Segurança Cibernética ("Política") consolida as regras aplicáveis ao uso dos equipamentos e de todos os recursos que envolvam tecnologia da informação da M. Safra & Co. (nome fantasia de AMS Capital Ltda. ("Empresa"), bem como sua utilização pelos sócios, administradores e funcionários da Empresa ("Colaboradores").

1.2. Esta Política visa, principalmente, preservar a boa ordem de funcionamento e conservação dos equipamentos eletrônicos e das informações da Empresa. Esta Política leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Empresa.

1.3. Regras adicionais e/ou mais específicas de segurança e de utilização dos recursos de tecnologia serão divulgadas pelo Departamento de Tecnologia ou pelo Comitê de Tecnologia ("Comitê de TI"), e estarão sempre disponíveis em locais de acesso comum na rede. Os Colaboradores observarão tais regras, responsabilizando-se pela manutenção da configuração original dos equipamentos que utiliza, sendo vedada qualquer modificação, salvo mediante expressa e prévia autorização do Departamento de Tecnologia ou pelo Comitê de TI.

II. IDENTIFICAÇÃO DE RISCOS *(RISK ASSESSMENT)*

2.1. No âmbito de suas atividades, a Empresa identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais (conforme definido no Código de Ética e Manual de *Compliance* da Empresa), incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Empresa, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- Sistemas: informações sobre os sistemas utilizados pela Empresa e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Empresa;

- Governança da Gestão de Risco: a eficácia da gestão de risco pela Empresa quanto às ameaças e planos de ação, de contingência e de continuidade de

negócios.

2.2. Ademais, no que se refere especificamente à segurança cibernética, a Empresa identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);

- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

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

2.3. Com base no exposto acima, a Empresa avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

III. AÇÕES DE PREVENÇÃO E PROTEÇÃO

3.1. Após a identificação dos riscos, a Empresa adota as medidas a seguir descritas para proteger suas informações e sistemas.

3.1.1. Propriedade das Informações e Equipamentos

3.1.1.1 O *hardware*, *software*, bancos de dados e demais equipamentos de telefonia e de informática são de propriedade da Empresa e/ou de terceiros que mantém contratos com a Empresa.

3.1.1.2 Além disso, os dados armazenados nos equipamentos da Empresa pertencem exclusivamente à Empresa e não podem ser copiados ou de outra forma transmitidos pelo Colaborador, a não ser para o estrito cumprimento de suas funções como colaborador da Empresa. Dentre tais dados incluem-se: toda e qualquer informação tangível ou intangível que tenham ou não sido desenvolvidas pelos Colaboradores (incluindo, mas não se limitando a todo tipo de propriedade intelectual, descobertas, ideias, invenções, conceitos, *know-how*, técnicas, desenhos, projetos, especificações, diagramas, amostras, fluxogramas, programas de computador, discos, *pen-drives*, fitas, modelos, projeções, nomes e informações sobre clientes, bom como quaisquer outras informações técnicas, financeiras ou comerciais, informações e dados relacionados a modelagem de dados, estratégias quantitativas, documentos, planilhas

eletrônicas, e quaisquer outras informações do banco de dados da Empresa). Em caso de desligamento do Colaborador, fica desde já acordado que o Colaborador estará proibido de manter em seu poder bem como fazer qualquer tipo de uso das informações e dados mencionados acima.

3.1.2. Acesso Escalonado do Sistema

3.1.2.1. O acesso como "administrador" de área de *desktop* será limitado aos usuários aprovados pelo Diretor de *Compliance* e Risco e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

3.1.2.2. A Empresa, ademais, mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente aqueles que contemplem Informações Confidenciais (conforme definido no Código de Ética e Manual de *Compliance*), de acordo com as funções e responsabilidades dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e *login* disponibilizados.

3.1.2.3. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Empresa em caso de violação.

3.1.3. *Hardware* e *Software*

3.1.3.1. Não deverão ser realizadas alterações no *hardware* e *software*, bem como é vedada a instalação de *software*, aplicativos, complementos ou *plugins,* de qualquer natureza sem autorização prévia do Departamento de Tecnologia ou do Comitê de TI.

3.1.3.2. Caso algum Colaborador pretenda instalar qualquer componente, periférico ou *software* em qualquer equipamento da Empresa, deverá encaminhar uma solicitação ao Departamento de Tecnologia, previa e formalmente, por meio de mensagem eletrônica endereçada ao tecnologia@msafra.com.br.

3.1.3.3. A atualização de qualquer *software* somente poderá ser realizada pelo Departamento de Tecnologia. Caso o Colaborador receba algum alerta de atualização ou solicitação de instalação, deverá comunicar tal fato imediatamente ao Departamento de Tecnologia, a menos que haja orientação específica, como por exemplo, a reinicialização após a aplicação automática de atualizações de segurança da Microsoft.

3.1.3.4. O Departamento de Tecnologia pode a qualquer momento, e sem prévio aviso, remover quaisquer *softwares* instalados que não façam parte das atividades da Empresa.

3.1.3.5. O uso de quaisquer equipamentos de propriedade particular, como por exemplo, *notebooks* e *smartphones*, e que utilizem recursos e mantenham conectividade com a rede de computadores da Empresa, dependerão da aprovação pelo Departamento de Tecnologia e estarão sujeitos às mesmas regras desta Política.

3.1.4. Senhas

3.1.4.1. A senhas de acesso aos equipamentos e sistemas são de caráter pessoal, e são intransferíveis, cabendo ao seu titular total responsabilidade quanto ao seu sigilo.

3.1.4.2. É vedado o compartilhamento de senhas de acesso, exceto nos casos expressamente autorizados pelo Departamento de Tecnologia ou Comitê de TI.

3.1.4.3. Os Colaboradores trocarão suas senhas de acesso de acordo com as políticas dos sistemas acessados e conforme instruído pelo Departamento de Tecnologia e a qualquer momento, imediatamente, quando julgar que tal senha não é de seu domínio exclusivo.

3.1.5. Arquivos

3.1.5.1. Todos os arquivos de trabalho deverão ser salvos em unidades e pastas na rede de acordo com o assunto ou departamento relacionado. Somente dessa forma será garantida a segurança, as permissões de acesso e *backups* realizados diariamente no período noturno. Arquivos não relacionados ao trabalho, como fotos e músicas, estarão sujeitos à exclusão sem prévio aviso.

Exemplo de unidades e pastas:
(T:\) Arquivos em Everest01
(U:\) Users em Everest01
(Z:\) “seu nome” em Everest01

3.1.5.2. Arquivos que forem salvos no disco local (C:\) do computador são de responsabilidade do próprio usuário e não terão *backup*.

3.1.6. Correio Eletrônico

3.1.6.1. O uso do correio eletrônico, seja no ambiente externo ou interno, deverá servir primordialmente para fins profissionais, estando expressamente vedadas mensagens que sejam contrárias à lei, à ética e aos bons costumes, como por exemplo, aquelas de conteúdo desabonador à Empresa, seus Colaboradores ou terceiros a eles relacionados; racista ou discriminatório; de estímulo a crimes, como o tráfico/uso de drogas e à violência em geral; político-partidário, similar a “correntes”; ou qualquer outro que possa ser considerado pejorativo ou proibido.

3.1.6.2. O correio eletrônico deve ser utilizado para o desenvolvimento pelo Colaborador de suas atribuições junto à Empresa, de maneira que a Empresa poderá monitorar, e se necessário, ler as mensagens eletrônicas enviadas e recebidas pelos Colaboradores. Tal monitoramento e leitura inclui a verificação das mensagens trocadas e a identificação daquelas, cujo conteúdo esteja em desacordo com a presente política e/ou outras políticas da Empresa, seja por envolver eventual compartilhamento de

informações confidenciais da Empresa ou que desrespeitem as regras dispostas nesta Política.

3.1.6.3. A Empresa poderá utilizar as mensagens enviadas e recebidas pelos Colaboradores da maneira como a Empresa entender necessário, inclusive em ações judiciais, administrativas e similares movidas no âmbito dos Poderes Judiciário e Executivo e seus respectivos órgãos, agências e cortes.

3.1.6.4. Os Colaboradores são proibidos de abrir mensagens não solicitadas (SPAM), que contenham anexos desconhecidos, que remetam a *websites* de conteúdos duvidosos ou qualquer outro tipo de mensagem que possa induzir ao erro e à inclusão de senhas e dados pessoais.

3.1.7. Internet

3.1.7.1. A *Internet* e todos os seus recursos deverão ser utilizadas unicamente para finalidades diretamente relacionadas às atividades de trabalho da função que os Colaboradores desempenhem junto à Empresa.

3.1.7.2. A Empresa poderá monitorar os acessos dos Colaboradores à *Internet,* podendo inclusive verificar os *websites* acessados, o tempo gasto na consulta e a frequência com que o Colaborador visita tais *websites*.

3.1.8. Mensagens Instantâneas

3.1.8.1. A Empresa não disponibiliza sistemas para troca de mensagens instantâneas, e, portanto, não se responsabiliza pela utilização de recursos próprios que utilizem aplicativos do tipo WhatsApp, Messenger ou qualquer outro similar, mesmo se utilizados dentro de suas dependências. Exceção feita aos sistemas que tiverem esse tipo de recurso específico e incorporados aos *softwares* oferecidos pela Empresa ao Colaborador, para exercício de suas funções, como por exemplo, as ferramentas de *chat* dos Terminais Bloomberg ou Thomson Reuters que possuem suas próprias políticas de segurança na geração de *logs* para armazenamento e registro das conversas.

3.1.9. Gravação de Telefones

3.1.9.1. A Empresa tem o direito e o dever de manter a gravação das conversas realizadas através das linhas telefônicas presentes nos equipamentos da mesa de operações financeiras, sejam linhas do PABX, ramais internos ou linhas privativas com terceiros.

3.1.9.2. Outros ramais e linhas telefônicas dos todos os Colaboradores também poderão, a qualquer momento, serem gravados conforme a Empresa julgue necessário.

3.1.10. Câmeras

A Empresa possui câmeras instaladas para monitorar todas as entradas as suas dependências e em alguns locais de circulação interna. As imagens são monitoradas e gravadas com a finalidade de controle da segurança do patrimônio e segurança física dos Colaboradores. Estas imagens pertencem exclusivamente à Empresa.

3.1.11. Acesso Remoto

3.1.11.1. A Empresa permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra:

(a) Os Colaboradores têm permissão para acessar o correio eletrônico a partir de aplicativos instalados em seus *smartphones* ou *tablets*, desde que mantenham em seus dispositivos pessoais *softwares* de proteção contra *malware*/antivírus.

(b) Ademais, os Colaboradores autorizados pela Diretoria a realizar acesso remoto a outras plataformas serão instruídos a (i) manter *softwares* de proteção contra *malware*/antivírus nos dispositivos remotos, (ii) relatar ao Diretor de *Compliance* e Risco qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Empresa e que ocorram durante o trabalho remoto, e (iii) não armazenar Informações Confidenciais (conforme definido no Código de Ética e Manual de *Compliance*) ou sensíveis em dispositivos pessoais.

IV. COMITÊ DE TI E DEPARTAMENTO DE TECNOLOGIA

4.1. O Departamento de Tecnologia é composto pelos Srs. Fábio Gentile e Elton Dias.

4.2. O Comitê de TI é composto pelo Diretor responsável pela área de *compliance*, pela Diretora Jurídica e pelo Gerente de Tecnologia.

V. MONITORAMENTO E TESTES

5.1. O Departamento de Tecnologia adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, semestral:

(i) Deverá monitorar, por amostragem, o acesso dos Colaboradores a *sites*, *blogs*, *fotologs*, *webmails*, entre outros, bem como os *e-mails* enviados e recebidos;

(ii) Deverá monitorar, por amostragem, as ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Empresa para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Empresa; e

(iii) Deverá verificar, por amostragem, as informações de acesso ao espaço do escritório, a *desktops*, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

VI. PLANO DE IDENTIFICAÇÃO E RESPOSTA

6.1. Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Empresa (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais (conforme definido no Código de Ética e Manual de *Compliance*), mesmo que de forma involuntária, deverá ser informada ao Departamento de Tecnologia prontamente. O Comitê de TI determinará quais membros da administração da Empresa e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Comitê de TI determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

6.2. Procedimentos de Resposta

O Departamento de Tecnologia responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Empresa de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais (conforme definido no Código de Ética e Manual de *Compliance*) de fundo de investimento sob gestão da Empresa, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial); e

(vii) Determinação do responsável (ou seja, a Empresa ou o cliente ou investidor

afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê de *Compliance*, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

VII. ARQUIVAMENTO DE INFORMAÇÕES

7.1. De acordo com o disposto neste Manual, os Colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro (conforme consta do Código de Ética e Manual de *Compliance* da Empresa), em conformidade com o inciso IV do Artigo 16 da Instrução CVM nº 558/2015, pelo prazo de 5 (cinco) anos ou superior, nas hipóteses exigidas pela legislação e regulamentação em vigor.

VIII. TREINAMENTO

8.1. O Comitê de TI organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de *compliance* (conforme consta do Código de Ética e Manual de *Compliance* da Empresa).

IX. REVISÃO DA POLÍTICA

9.1. O Comitê de TI deverá realizar uma revisão desta Política anualmente, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Empresa e acontecimentos regulatórios relevantes.

Vigente a partir de janeiro de 2019. Alterada em outubro de 2019.

Declaro que li, concordo, e me obrigo a observar as Diretrizes para Negociação e Investimentos da M. Safra & Co.:

Colaborador:

_____

Nome:
Data:

ANEXO III

MODELO DE TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/MF sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **AMS Capital Ltda.** ("AMS") por prazo indeterminado:

[ ] ou até que me certifique pela CGA;

[ ] ou caso o Conselho de Certificação, nos termos do Art. 17 do Código de Certificação, me conceda a isenção de obtenção da CGA;

[ ] tendo em vista que não sou mais Colaborador da AMS;

[ ] já que não tenho alçada/poder discricionário de decisão de investimento.

São Paulo, [•] de [•] de [•].

_____

[**Colaborador**]

_____

AMS Capital Ltda

Testemunhas:

1._____
Nome:
CPF:

2._____
Nome:
CPF: