



Prezados Colaboradores,

Primeiramente, gostaríamos de estabelecer algumas informações que serão de grande importância no desenvolvimento de nossas atividades. Pautamos nossos negócios com base na ética, na moral e em respeito às normas legais. Para tanto, é necessário seguir as regras contidas nesta cartilha de orientação de conduta, sempre almejando manter os padrões elevados de profissionalismo e seriedade. A nossa reputação, dentro do mercado em que atuamos é muito importante e a responsabilidade de todos é zelar para que ela não seja denegrida ou, de qualquer forma, desgastada.

Em seguida, cumpre mencionar que nossa empresa atua de forma independente e segregada de qualquer outra sociedade. O exercício e alcance de nossos objetivos sociais, pauta-se nos princípios éticos e morais, sempre em consonância com os preceitos legais vigentes.

Dessa forma, elaboramos a presente Cartilha de Conduta, cujo conteúdo deve ser fielmente observado por todos os colaboradores da Sociedade, assim entendidos seus (i) sócios; (ii) funcionários; (iii) diretores; (iv) estagiários; ou (v) quaisquer pessoas que, em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações relevantes sobre a Sociedade ou sobre suas estratégias de investimento.

Todo o abaixo exposto deverá ser compulsoriamente observado pelos colaboradores da Sociedade, declarando estarem cientes de todas as regras e políticas aqui expostas, que lhes foram previamente apresentadas pelo responsável pelo compliance da Sociedade e em relação às quais não existe qualquer dúvida, comprometendo-se a observá-las a todo tempo no desempenho de suas atividades.



## Sumário

NORMAS DE CONDUTA .....	3
1. Informações privilegiadas .....	4
2. Conceito “need to know” .....	4
3. Informações confidenciais em geral .....	5
4. Dever de Sigilo .....	5
5. Conflitos de Interesse .....	6
6. A Política de <i>Chinese Wall</i> e outras barreiras de informação .....	7
7. Limitando o fluxo de informações .....	7
8. Segurança da Informação: .....	7
8.1. Acesso às informações e equipamentos: .....	7
8.2. Política de senhas .....	8
8.3. Acesso Remoto .....	9
8.4. Manuseio e Descarte de Documentos Impressos .....	9
8.5. Utilização de e-mails, internet e redes sociais .....	9
8.6. Política de backups .....	10
8.7. Outras recomendações .....	10
9. Política de seleção e contratação de prestadores de serviço: .....	11
10. Política Anticorrupção .....	11
10.1. Pagamentos facilitadores .....	12
10.2. Solicitação de doações .....	12
10.3. Lidando com funcionários públicos .....	13
10.4. Doações políticas e ações de lobby .....	13
10.5. Política de presentes e entretenimento .....	14
10.5.1. Presentes para as pessoas .....	14
10.5.2. Presentes de pessoas .....	14
11. Utilização de bens e equipamentos .....	15
12. Propriedade Intelectual: .....	16
13. Programa de Treinamento .....	16
14. Comunicação com a Imprensa .....	17
15. Controles Internos .....	18
PENALIDADES .....	19



## NORMAS DE CONDUTA

### Princípios norteadores das condutas:

Todos os colaboradores da Sociedade deverão pautar suas condutas em conformidade com os valores da boa-fé, lealdade, transparência, diligência e veracidade, evitando quaisquer práticas que possam ferir a relação fiduciária mantida com os investidores.

Todos os esforços em prol da eficiência na gestão dos fundos e carteiras devem visar à obtenção do melhor retorno aos investidores, com base na análise e interpretação de informações divulgadas ao mercado, e jamais no acesso a informações privilegiadas. Os colaboradores deverão observar as regras e procedimentos internos relacionados a forma e prazos de arquivamento de toda a documentação relativa às operações envolvendo títulos e valores mobiliários, inclusive aquelas relacionadas ao processo de tomada de decisão de investimento, conforme orientações do compliance.

Os colaboradores da Sociedade devem estar conscientes de que a informação transparente, precisa e oportuna constitui o principal instrumento à disposição do público investidor para que lhes seja assegurado o indispensável tratamento equitativo. As informações prestadas ao investidor não devem, de forma efetiva ou aparente, assegurar a existência de resultados futuros ou a isenção de riscos do investimento.

O relacionamento dos colaboradores da Sociedade com os participantes do mercado e com os formadores de opinião deve dar-se de modo ético e transparente.

A Sociedade transferirá às carteiras sob gestão qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de administradora de carteiras de valores mobiliários, observadas as exceções previstas em norma específica.

Os colaboradores deverão informar ao responsável pelo compliance sempre que se verifique, no exercício de suas atribuições, a ocorrência de violação à legislação ou às normas internas de conduta.

Sem prejuízo do acima estabelecido, os colaboradores deverão atentar-se aos seguintes padrões de conduta no desempenho das suas atividades:



- a) não fazer propaganda garantindo níveis de rentabilidade, com base em desempenho histórico da carteira ou de valores mobiliários e índices do mercado de valores mobiliários;
- b) não fazer quaisquer promessas quanto a retornos futuros;
- c) não negociar títulos e valores mobiliários com a finalidade de gerar receitas de corretagem ou de rebate para si ou para terceiros; e
- d) não negligenciar, em qualquer circunstância, a defesa dos direitos e interesses do cliente/investidor.

## 1. Informações privilegiadas

Em caso de acesso a informações privilegiadas, entendendo-se por informações privilegiadas aquelas cujo conteúdo seja confidencial e não-público, assim como qualquer material que possa influenciar preços no mercado, não poderá, recomendar, comprar ou vender valores mobiliários ou instrumentos financeiros que possam ter seus preços afetados pela informação. Adicionalmente, também não poderá de nenhuma forma transmitir informações privilegiadas, de forma direta ou indireta.

Adicionalmente, espera-se dos colaboradores que estes advirtam, de forma clara, àqueles em relação a quem se verificar a necessidade de revelar informação privilegiada, sobre a responsabilidade pelo cumprimento do dever de sigilo e pela proibição legal de que se utilizem de tal informação para obter, em benefício próprio ou alheio, vantagem mediante negociação com tais títulos e/ou valores mobiliários.

Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, procurar o responsável pelo compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva ao conceito de informação confidencial definido acima.

## 2. Conceito *"need to know"*

Eventualmente, no desempenho de suas funções na sociedade você terá acesso recorrente a diversas informações confidenciais sobre a sociedade, seus clientes, fornecedores e colaboradores, sendo proibida a utilização ou divulgação destas informações, ainda que após o seu desligamento. Tome cuidado e considere como confidencial as informações que você



armazena em formato escrito, verbal ou eletrônico, e ainda que você esteja autorizado a divulgá-las só o faça para aquelas pessoas que realmente necessitam saber (conceito de “need to know”).

Recomendamos cuidados com o uso de e-mails e internet em geral, especialmente no tocante à utilização e processamento de informações confidenciais por estes meios.

### **3. Informações confidenciais em geral**

Sempre que você repassar ou comunicar informações confidenciais a terceiros autorizados a recebê-las, tenha certeza de que esta pessoa tem consciência de que estas informações são confidenciais e de como deve ser seu tratamento. Em certos casos, será necessário que seja assinado um acordo de confidencialidade.

A revelação de informação confidencial só será permitida quando necessária para a Sociedade conduzir seus negócios de maneira eficaz e, ainda, somente se não houver motivos ou indícios para presumir que o receptor da informação a utilizará erroneamente.

O fornecimento de informações confidenciais a pessoas externas à Sociedade será realizado somente nos casos estritamente necessários a fim de cumprir as normas atinentes à atividade desenvolvida pela Sociedade, proteção contra fraudes ou qualquer outra atividade ilegal suspeita, mediante contratos de confidencialidade, quando for o caso.

### **4. Dever de Sigilo**

Os Colaboradores devem guardar absoluto sigilo sobre toda e qualquer informação de natureza confidencial a que tenham acesso ou conhecimento no desempenho de suas funções, inclusive por meio dos sistemas e arquivos disponibilizados pela sociedade incluindo a proteção pela equipe de gestão dos algoritmos a que tiverem acesso na administração das carteiras. Tal determinação se aplica igualmente às informações obtidas/repasadas verbal ou informalmente, assim como às escritas ou impressas.

Sob nenhuma circunstância as pessoas vinculadas à Sociedade poderão utilizar informações confidenciais para obter vantagens pessoais, tampouco poderão fornecê-las para terceiros, inclusive familiares, parentes e amigos, ou mesmo a outras pessoas vinculadas à sociedade que não necessitem de tais informações para executar suas tarefas.



A revelação dessas informações a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada ao diretor responsável pela gestão para que este decida sobre a forma mais adequada para tal revelação.

## 5. Conflitos de Interesse

Consideram-se conflitos de interesse, de forma genérica e não limitadamente, quaisquer interesses pessoais dos colaboradores, em benefício próprio ou de terceiros, contrários ou potencialmente contrários aos interesses da Sociedade, dos investidores dos fundos e demais veículos de investimento geridos pela Sociedade e dos demais clientes da Sociedade.

Como colaborador da sociedade você deve sempre evitar que seus interesses conflitem ou passem a ideia de conflitar com os interesses da empresa, sendo que qualquer circunstância deste tipo, ainda que potencial, deve ser imediatamente comunicada aos seus superiores. Para casos em que seus relacionamentos pessoais ou profissionais possam, ainda que de forma não intencional, criar conflitos de interesse, comunique estas situações assim que identificadas para que seja possível evitar a tempo qualquer dano à empresa ou ao seu trabalho.

Os colaboradores da Sociedade devem evitar desempenhar outras funções fora da Sociedade que possam gerar conflitos de interesse, ou mesmo aparentar tais conflitos. Também devem evitar defender interesses de terceiros que possam gerar conflitos de interesse na tomada de decisão e implicar em algum tipo de prejuízo para a Sociedade ou seus investidores.

Quaisquer transações em nome da Sociedade com pessoas físicas ou jurídicas com as quais qualquer dos colaboradores da Sociedade ou pessoa a este ligada possua interesse financeiro devem sempre ser previamente autorizadas pelo compliance para a devida aprovação a fim de evitar potenciais conflitos de interesse.

Caso o colaborador resolva exercer outras atividades, sejam elas com ou sem fins lucrativos, além da praticada junto à Sociedade, deve comunicar previamente ao responsável pelo compliance para a devida aprovação a fim de evitar potenciais conflitos de interesse.

Caberá ao compliance orientar a estrutura de governança da Sociedade, visando garantir a segregação de atividades no âmbito interno e evitando conflitos de interesse, ainda que



potenciais, entre as atividades desenvolvidas pelos colaboradores na instituição ou empresas ligadas.

## 6. A Política de *Chinese Wall* e outras barreiras de informação

De forma a barrar o fluxo de informações entre as áreas que lidam com informações privilegiadas e aquelas que negociam títulos e valores mobiliários, foi criada a Política de *Chinese Wall*, que nada mais é do que a efetiva restrição/proibição do fluxo de informações privilegiadas entre qualquer área da sociedade ou fora dela.

Esta proibição de fluxo de informação deve ser rigorosamente respeitada não só entre áreas distintas da sociedade para a qual você se dedica como em relação a empresas ligadas ou que venham a funcionar em áreas contíguas. Certifique-se, sempre, que não há risco de vazamento das informações confidenciais e/ou privilegiadas, protegendo-as e restringindo sua circulação.

## 7. Limitando o fluxo de informações

Para restringir o fluxo inadequado de informações, barreiras são impostas de várias formas. O isolamento físico, procedimental ou ainda eletrônico são formas utilizadas pela Sociedade para barrar a disseminação de informações privilegiadas e sigilosas. Ainda assim, a Sociedade adota treinamento interno dos seus colaboradores visando, dentre outras questões, disseminar a cultura de compliance e ratificar a importância de manutenção da confidencialidade das informações com as quais a Sociedade e seus colaboradores lidam no desempenho das suas funções.

## 8. Segurança da Informação:

Os colaboradores da Sociedade que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

O sistema eletrônico utilizado pela Sociedade está sujeito à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

### 8.1. Acesso às informações e equipamentos:

Todos os computadores da Sociedade possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por



peessoas não autorizadas. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores utilizados pela Sociedade permitem a identificação do seu remetente/receptor.

Os dados da Sociedade são protegidos por políticas de permissionamento de acesso às pastas do servidor. Cada colaborador somente tem acesso aos dados pertinentes às suas funções. Os colaboradores devem garantir que a segurança da rede interna seja mantida pelo uso adequado de senhas.

Além do permissionamento, os arquivos mais importantes estão encriptados e as estações de trabalho ficam bloqueadas na ausência dos respectivos colaboradores.

Não é permitido salvar cópia de informações confidenciais em computadores pessoais ou outros dispositivos eletrônicos que não sejam disponibilizados pela Sociedade, a não ser com a expressa autorização do Compliance.

Todas as atividades efetuadas utilizando os meios de comunicação e ferramentas de trabalho disponíveis na Sociedade podem ser monitoradas e armazenadas sem notificação prévia.

O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física da equipe de gestão de recursos de terceiros.

## 8.2. Política de senhas

Todos os computadores devem ter uma senha não trivial para ser acessado. Essa senha deve ser conhecida apenas pelas pessoas que usam aquele computador.

Todos os e-mails devem ter senhas complexas, marcadas como “Strong” pelo gmail. De preferência com autenticação de 2 fatores. Se o e-mail for colocado no telefone, este deve ter senha para ser desbloqueado (há uma configuração no domínio que exige essa senha para habilitar o e-mail).

Senhas do computador devem contabilizar pelo menos 10 horas no site <https://howsecureismypassword.net/>. Caso a senha seja tentada 5 vezes de forma errada, a conta ficará bloqueada por 5 minutos.

Senhas de planilhas sensíveis: Devem contabilizar mais de 1 milhão de anos no site <https://howsecureismypassword.net/>





Nossa equipe de TI deve ser consultada para esclarecimento de qualquer dúvida relacionada aos requisitos de segurança acima descritos.

### 8.3. Acesso Remoto

Somente é permitida a instalação de software de acesso remoto em casos de grande necessidade. Caso seja necessário acessar esporadicamente o seu próprio computador de maneira remota, use uma versão *portable* (que não fica rodando o tempo todo).

Somente inicie o programa quando for acessar um computador remoto ou se for preciso acessar o seu computador remotamente. Caso precise acessar o seu computador em um horário que ninguém está no escritório, deixe o programa ligado. Caso contrário, mantenha desligado. Quanto mais tempo o programa ficar ligado, maior a chance de alguém descobrir a sua senha e usar o programa para controlar o computador. Preferencialmente, exclua ele da inicialização automática.

É essencial uma senha forte para este tipo de programa. A senha é a sua única proteção. Ainda que seja preciso alguém descobrir o seu ID, não é difícil fazer um robô que fique tentando repetidas vezes. É mais fácil descobrir se um ID é válido caso o programa estiver rodando. Teste sua senha no site: <https://howsecureismypassword.net/>

Não abuse deste tipo de acesso. Ele é uma vulnerabilidade séria e ele dá acesso a todo o seu computador e a todas as pastas da nossa rede que você tem acesso. Tenha isso em mente quando decidir usar este tipo de ferramenta.

### 8.4. Manuseio e Descarte de Documentos Impressos

Os colaboradores têm a obrigação de garantir a segurança das cópias impressas de informações confidenciais utilizadas dentro ou fora das dependências da Sociedade.

Todo e qualquer papel ou documento com dados confidenciais, estratégicos ou até dados pessoais dos colaboradores devem ser triturados na picotadora de papel disponível no escritório da Sociedade.

### 8.5. Utilização de e-mails, internet e redes sociais



Todos os assuntos de negócios devem ser conduzidos somente pelo sistema de correio eletrônico / mensagens instantâneas da Sociedade e não por contas de e-mail pessoal ou redes sociais.

É proibido comentar, publicar ou discutir assuntos referentes à Sociedade, seus clientes e sócios, ou prestar informações estratégicas, inclusive de investimento, em qualquer meio de comunicação das mídias sociais, sem a aprovação prévia e formal do Compliance.

A internet deverá ser utilizada de maneira profissional. É proibido o acesso a sites ou o envio de mensagens eletrônicas de conteúdo inapropriado, ilegal, ofensivo ou discriminatório. Fica vedado também o repasse de mensagens eletrônicas com conteúdo provocativo a uma pessoa ou a um grupo de pessoas.

#### **8.6. Política de backups**

Como descrito no Plano de Continuidade de Negócios da Sociedade, esta possui uma política de backup bastante abrangente que assegura o restabelecimento operacional da empresa em curto espaço de tempo.

Todos os documentos arquivados nos computadores da Sociedade são objeto de back-up com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

#### **8.7. Outras recomendações**

Todos os computadores devem ser bloqueados quando não estiverem sendo utilizados. Computadores pessoais devem ser bloqueados no máximo 30 minutos de inatividade. Computadores compartilhados devem ser bloqueados no máximo após 1 hora de inatividade. Esta política é configurada por padrão no servidor de domínio. Ou seja, apesar de o usuário poder mudá-la, a configuração padrão será de 30 minutos.

Todos os computadores devem ter um antivírus atualizado e rodando o tempo todo. Caso seja necessário desligá-lo por algum motivo, sempre colocar um tempo pequeno para que ele seja reativado.

Cuidado com e-mails falsos. Especialmente e-mails que peçam dados sensíveis da empresa. Mesmo que o remetente seja real, é importante ter certeza de que os dados são necessários.



Ataques deste tipo (*spear fishing*) são comuns em gestoras, pois elas podem ter acesso privilegiado a rede dos bancos/corretoras/bolsa.

Os anexos dos e-mails não devem ser abertos a menos que se tenha certeza absoluta do que se trata. Arquivos que não sejam documentos simples (pdf, doc, xls, etc) não devem ser abertos sem antes fazer uma varredura adicional do antivírus. Atenção especial para arquivos zip e exe. Caso não se tenha muita certeza da procedência do e-mail e seja necessário olhar o anexo, fazer através do Gmail online. Por lá eles podem varrer o anexo antes de abrir.

Não é permitido compartilhar diretamente pastas nos computadores. Todos os arquivos que precisam ser compartilhados devem ficar na rede. Caso não haja um lugar adequado, falar com o administrador de rede para que um seja criado

#### **9. Política de seleção e contratação de prestadores de serviço:**

Os colaboradores devem cultivar padrões elevados de qualidade de serviço na Sociedade, evitando a contratação de pessoas de reputação não ilibada ou que possam, de qualquer forma, prejudicar a imagem e reputação da instituição.

A contratação de prestadores de serviço em nome da Sociedade deve sempre ser precedida de análise crítica que avalie, além da qualidade do produto / serviço, sua idoneidade.

O preço cobrado pelo serviço deve ter um custo benefício atraente, em comparação com a média do mercado, utilizando para tal, a comparação dos preços cobrados por diferentes concorrentes.

A contratação de pessoas naturais residentes ou entidades constituídas em países que não aplicam ou aplicam insuficientemente as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo – GAFI, assim como pessoas politicamente expostas, indivíduos que ocupam ou ocuparam posições públicas, tais como: funcionários do governo, executivos de empresas governamentais, políticos, funcionários de partidos, assim como seus parentes e associados devem sempre passar por aprovação do compliance.

#### **10. Política Anticorrupção**

A Kadima Gestão de Investimentos não paga ou promete suborno para melhorar a performance de seus negócios e não aceita que colaboradores ou terceiros contratados



realizem este tipo de atividade. Corrupção é crime e está sujeita à penalidade legal. A gestora não tolerará nenhuma situação de suborno e/ou qualquer modalidade de outros atos de corrupção.

Atos de corrupção não se resumem ao pagamento de propina, podendo se caracterizar por troca de presentes ou favores, concessões de empréstimos ou a prestação de serviços para aqueles que estão sendo subornados. A Kadima possui contratos de serviços profissionais que resultam em pagamentos a diversas instituições financeiras, consultores profissionais, terceirizados e outros. Por isso, é muito importante considerar a natureza de qualquer outro benefício oferecido por terceiro conectado com uma relação profissional, visto que pode ser considerado um agradecimento inadequado para negócios passados ou uma tentativa de influenciar negócios futuros. No entanto, reconhecemos que existem presentes modestos, entretenimento ou outros benefícios que são dados para pessoas e não causariam as mesmas preocupações de improbidade, conforme já previsto em nossos manuais de compliance e de conduta.

A presente Política não pretende proibir a entrega ou aceitação de itens promocionais e de boa-fé.

### **10.1. Pagamentos facilitadores**

Nenhum pagamento facilitador deve ser feito por ou em nome da gestora. Pagamentos facilitadores são pagamentos de baixo ou médio valor financeiro feitos para garantir ou acelerar as ações de rotina ou, de outra forma, induzir funcionários públicos ou terceiros a realizar funções de rotina que são obrigados a realizar, como emissão de licenças ou liberação bens retidos em alfândega. Este tipo de pagamento não inclui taxas administrativas legalmente aplicáveis aos negócios da gestora.

### **10.2. Solicitação de doações**

É proibido solicitar doações de fornecedores que leve ao entendimento de que o cumprimento é condição essencial para negócios futuros com a Kadima. Encorajamos os nossos colaboradores a contribuir com seu tempo e seus recursos pessoais para instituições de caridade. No entanto, a menos que a solicitação seja apoiada pela gestora, é proibido utilizar o nome ou material de papelaria da Kadima para esta finalidade. Todos os pedidos de presentes corporativos para instituições de caridade devem ser encaminhados ao departamento de compliance.



### 10.3. Lidando com funcionários públicos

Não faça promessas, pagamentos ou autorize qualquer presente de valor em nome da gestora, direta ou indiretamente, para funcionários públicos, nacionais ou estrangeiros, para obter ou reter negócios, garantir uma vantagem ou influenciar um funcionário público no desempenho da sua função oficial.

A doação de presentes ou outros benefícios a funcionários públicos ou a instituições de caridade que possuam vínculo com funcionários públicos pode ser interpretada como ato de suborno ou forma de influenciar decisões em favor da gestora, não importando o valor do presente. Muitos países, estados e jurisdições locais possuem leis que restringem presentes, por exemplo, refeições, entretenimento, transporte, alojamento ou demais coisas de valor, que podem ser fornecidos a funcionários públicos nacionais ou estrangeiros, o que inclui qualquer pessoa empregada por ou representante do governo, funcionário público de partido político, funcionários públicos de organizações internacionais públicas e candidatos a cargos públicos.

O termo “funcionário público” inclui pessoas eleitas ou nomeadas que detêm posições legislativas, administrativas ou judiciais como políticos e juizes. Também inclui pessoas que desempenham funções públicas, tais como, profissionais das agências de saúde pública, autoridades sanitárias, funcionários de planejamento e agentes de organizações públicas internacionais. A denominação “funcionário público” pode incluir os funcionários das empresas estatais, inclusive os fundos de riqueza soberana. Por exemplo, se um governo possui participação societária em um determinado banco e controla as atividades deste banco, os funcionários do banco devem ser considerados “funcionários públicos”.

Pagamentos efetuados indiretamente por meio de um consultor, contratado, ou outro intermediário também são proibidos por estas leis. Em nenhuma circunstância pode-se oferecer algo de valor para um funcionário público com a finalidade de influenciá-lo a tomar ou abster-se de tomar qualquer ação oficial, ou induzi-lo a realizar negócios com a Kadima.

No caso de dúvidas ou preocupações em relação às leis referentes ao suborno e corrupção, o colaborador deve consultar o departamento de compliance.

### 10.4. Doações políticas e ações de lobby

Não ofereça contribuições, presentes ou outros benefícios para partidos políticos que possam influenciar, direta ou indiretamente, ou serem considerados influentes em uma decisão de negócios, sem as devidas aprovações.



Existem leis que regulam doações políticas no Brasil e em outros países. Dessa forma, para garantir que não ocorra violação a estas leis, todas as doações políticas, em nome da Kadima, devem ser anteriormente aprovadas, formalmente, pelo Comitê Executivo.

Não se envolva em qualquer atividade de lobby em nome da Kadima sem autorização específica.

### **10.5. Política de presentes e entretenimento**

Utilize o bom senso para dar ou receber presentes e o faça somente em circunstâncias limitadas.

Dar presentes, tais como: refeições, entretenimento, viagens, objetos é considerado uma forma de cortesia muito comum nos negócios das empresas. No entanto, as leis anticorrupção proíbem e punem severamente o ato de oferecer ou receber itens de valor a qualquer pessoa, instituição pública ou privada, com objetivo de obter vantagens pessoais ou de negócios.

Os colaboradores que não cumprirem com os requisitos estabelecidos neste código podem ser obrigados a devolver o valor de todos os presentes ou benefícios que recebam em nome da Kadima. Além disso, as violações das políticas da gestora, ou de exigências legais e regulamentares, podem resultar em medidas disciplinares e legais cabíveis, inclusive demissão.

#### **10.5.1. Presentes para as pessoas**

Os colaboradores cuja natureza do negócio demande podem oferecer presentes modestos, brindes e entretenimento, que tenham uma relação de negócios com a gestora. Por exemplo, é aceitável levar um cliente para almoçar, mas não é razoável que o evento não possua nenhuma ligação com o negócio a ser tratado. Ressaltamos que é vedada a oferta de qualquer quantia financeira a clientes.

#### **10.5.2. Presentes de pessoas**

Nenhum pagamento em dinheiro deve ser feito ou recebido por colaboradores da Kadima. Além disso, não é permitido dar, prometer ou receber presentes de funcionários públicos.



Os colaboradores não estão autorizados a dar nem receber itens caros, tais como: viagens, inscrições em conferências, custos de hospedagem ou patrocínios de evento, sem autorização prévia da diretoria do Compliance.

Consideramos aceitável receber brindes, presentes, entretenimento ou outros benefícios de pessoas realizando ou procurando realizar negócios com a Kadima, desde que os benefícios oferecidos ao colaborador não excedam a quantia limite de R\$ 250,00 e que não sejam recorrentes da mesma pessoa ou empresa. Valores acima deste limite devem sempre ser comunicados ao compliance para a devida aprovação a fim de evitar potenciais conflitos de interesse.

Brindes promocionais de baixo valor são permitidos desde que contenham a identificação do fornecedor ou cliente. Em caso de dúvida, o colaborador deve aconselhar-se com o compliance.

## 11. Utilização de bens e equipamentos

O patrimônio da Sociedade deverá ser utilizado exclusivamente para a consecução do seu objeto social, sendo dever de todos os colaboradores a sua preservação e utilização adequada.

Para fins de controle e segurança, todas as ligações poderão ser monitoradas e até mesmo gravadas.

Ligações telefônicas particulares são permitidas, desde que observado o bom-senso, sendo recomendada a ligação para telefones fixos, prioritariamente. A utilização de telefones celulares particulares é permitida, devendo ser mantida ao mínimo necessário.

Os colaboradores deverão utilizar os recursos de acesso à internet e serviço de correio eletrônico (e-mail) apenas para assuntos corporativos, sendo a utilização para fins particulares tratadas como exceção. Para preservar esses recursos, a Sociedade se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

O uso da rede para armazenar os arquivos pessoais é permitido, desde que a pasta seja corretamente identificada, ficando o colaborador ciente de que não será assegurada privacidade às informações armazenadas, as quais poderão ser acessadas por quaisquer colaboradores que possuam acesso à rede.

Os colaboradores não poderão utilizar os ativos da Sociedade para:



- (i) visitar sites na internet que contenham materiais obscenos, lascivos, preconceituosos ou outro tipo de material repreensível;
- (ii) enviar ou receber material obsceno ou difamatório ou cujo objetivo seja aborrecer, assediar ou intimidar terceiros;
- (iii) objetivar fins ilícitos;
- (iv) apresentar opiniões pessoais como se fossem da Sociedade.

## 12. Propriedade Intelectual:

Todos os documentos, arquivos, modelos, metodologias, fórmulas, cenários, projeções, análises e relatórios produzidos e desenvolvidos na realização das atividades da Sociedade ou a elas diretamente relacionadas, têm sua propriedade intelectual atribuída à Sociedade.

Ressalvada autorização expressa e por escrito do compliance da Sociedade, a exportação, o envio a terceiros, a cópia, descrição, utilização ou adaptação fora do ambiente da Sociedade, em qualquer circunstância, de qualquer item sujeito à propriedade intelectual da Sociedade são vedadas, sujeitas à apuração de responsabilidades nas esferas cível e criminal.

Uma vez rompido o vínculo de subordinação, o ex-colaborador da Sociedade permanece obrigado a observar as restrições mencionadas acima, sujeito à responsabilização pela via judicial.

## 13. Programa de Treinamento

A Sociedade conta com um programa de treinamento dos colaboradores que tenham acesso a informações confidenciais ou participem do processo de decisão de investimento dividido em 2 (duas) etapas distintas.

A primeira etapa consiste na apresentação pelo responsável pelo compliance dos normativos internos ao colaborador no ato do seu ingresso na Sociedade, disponibilizando-se para prestar quaisquer esclarecimentos que se façam necessários, e recolhendo o termo de adesão aos manuais e políticas pertinentes, os quais ficarão arquivados na sede da Sociedade em meio eletrônico ou digital.





Já a segunda etapa do treinamento ocorre anualmente quando o responsável pelo compliance, além de ratificar o conteúdo dos normativos internos e recolher a adesão aos manuais pertinentes, abordará as seguintes questões:

- Risco de imagem e risco legal (Descumprimento da legislação/regulamentação).
- Enforcement - Implicações da não observância das normas de conduta e ética.
- Boas práticas para manipulação da informação e utilização indevida de informações privilegiadas.
- Segregação de atividades de forma a evitar possíveis conflitos de interesses.
- Política de segurança e preservação da Informação, conceito "need to know".
- Identificação e comunicação das operações atípicas/suspeitas.
- Segregação entre a gestão de recursos próprios e de terceiros – política de investimentos próprios.
- Obrigações e responsabilidades dos demais prestadores de serviços correlatos: administrador fiduciário / distribuidores / custodiante / auditor independente.
- Gerenciamento dos limites operacionais e de risco e enquadramento às políticas de investimento das carteiras sob gestão.
- Metodologia adotada para a contabilização de ativos.
- Regras de aplicação, resgate, carência e conversão de cotas. Liquidez dos ativos X regras de movimentação previstas em regulamento.
- Política de voto em assembleias;
- Plano de Continuidade de Negócios;
- Política de Prevenção e Combate à Lavagem de Dinheiro;
- Melhores práticas no processo de seleção e contratação de parceiros e prestadores de serviço;
- Utilização dos bens e equipamentos da Sociedade;
- Processo de Suitability.

O compliance poderá promover treinamentos em periodicidade menor, visando à atualização e ampliação do conhecimento dos colaboradores acerca de novidades normativas e regulatórias, bem como discutir casos concretos ocorridos dentro e fora da instituição.

#### 14. Comunicação com a Imprensa

Visando ao resguardo dos interesses da Sociedade em face ao volume de informações com as quais precisa lidar diariamente, somente os diretores responsáveis pela gestão e distribuição, ou pessoa por estes prévia e expressamente autorizada, em quaisquer dos casos acompanhado pelo responsável pelo compliance, pode manter qualquer tipo de comunicação, em nome da



Sociedade, com jornalistas, repórteres, entrevistadores ou agentes da imprensa falada ou escrita (“Imprensa”).

Considera-se comunicação, para os fins da vedação estabelecida na cláusula anterior, a revelação à Imprensa de qualquer informação, principalmente as relacionadas a investidores, carteiras administradas e operações realizadas ou em desenvolvimento, obtidas no exercício das atividades da Sociedade, bem como de qualquer item sujeito à propriedade intelectual da Sociedade.

Os colaboradores da Sociedade autorizados a participar de entrevistas e assemelhados deverão restringir-se a tecer comentários estritamente técnicos, evitando o uso de juízos de valor desnecessários, devendo pautar suas declarações na cautela.

É vedado, sob qualquer circunstância, conceder declaração à Imprensa que possa aparentar ou ter conteúdo discriminatório em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei, assim como a utilização de expressões de baixo calão ou não condizentes com a melhor educação.

## 15. Controles Internos

O compliance visa fomentar a credibilidade e a sustentabilidade da Sociedade por meio da criação, implementação e monitoramento de rotinas e controles internos, os quais deverão colaborar para a mitigação de riscos de imagem, redução do impacto de eventuais riscos operacionais, geração de valor e longevidade da Sociedade.

A Sociedade conta com um profissional responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos, cujas atribuições e rotinas, sem prejuízo das responsabilidades indicadas neste Manual, estão previstas no Manual de Compliance.

Aos profissionais atuantes na área de compliance e controles internos deverá ser assegurado o amplo e irrestrito acesso a toda e qualquer informação, de cunho confidencial ou não.



## PENALIDADES

O não cumprimento das normas acima descritas pode ensejar penalidades ao colaborador. O teor destas penalidades será determinado pelo Comitê Executivo da Gestora e poderá variar desde advertência por escrito até a demissão por justa causa do colaborador, sem prejuízo de eventuais ações civis e penais que sejam pertinentes.

*Ciência do Colaborador:*

*Data:* \_\_\_\_/\_\_\_\_/\_\_\_\_

*Nome:*

\_\_\_\_\_