KX Ventures LTDA

POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS e SEGURANÇA DA INFORMAÇÃO

V001

POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS e SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE MODIFICAÇÕES DO DOCUMENTO			
Data	**Responsável**	**Versão**	**Alterações/Inclusões**
04/04/2025	**Diretor de Compliance e Riscos**	**001**	**Criação da Política**

A Política de Regras, Procedimentos e Controles Internos, incluindo Política de Confidencialidade, Segurança da Informação e Programa de Treinamento ("Política") tem caráter permanente. O conteúdo deste documento será constantemente revisto e atualizado, podendo ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da KX Ventures LTDA, sociedade limitada inscrita no CNPJ/MF sob o nº 53.069.721/0001-14 ("Gestora") e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações. Os destinatários da presente Política deverão preservar a confidencialidade de informações relativas aos negócios da Gestora sujeitas à presente Política, conforme aplicável.

1. INTRODUÇÃO

Este documento tem como objetivo estabelecer regras, procedimentos e descrição dos controles internos da Gestora, tendo em vista sua atuação como gestor de recursos de terceiros, cujo mercado é altamente regulado, de modo a garantir o permanente atendimento às normas, políticas e regulamentação vigente, referentes às diversas modalidades de investimento, à própria atividade de gestão de recursos de terceiros e aos padrões ético e profissional.

A presente Política aplica-se a todos os níveis hierárquicos da Gestora: sócios, administradores, empregados, consultores, prestadores de serviço, trainees, estagiários e demais colaboradores ("Colaboradores"). Todos os Colaboradores têm o conhecimento, a compreensão desta Política e estão cientes de que devem conhecer e respeitar todas as normas aqui dispostas. O descumprimento de tais normas poderá acarretar a imposição pelo Diretor de Compliance e Riscos das seguintes sanções administrativas a depender do grau de gravidade da conduta: (i) assinatura de termo de compromisso; (ii) advertência escrita ou verbal; (iii) censura; (iv) suspensão; ou (v) demissão/término da relação contratual.

2. PROCEDIMENTOS E CONTROLES INTERNOS

2.1. RESPONSABILIDADE DOS ENVOLVIDOS

Diretores da KX

Entende-se por diretores da Gestora aquelas pessoas físicas, sócios ou não, nomeadas em contrato social ("Diretores"), os quais possuem as seguintes funções:

- Aprovar esta Política.
- Acompanhar os resultados das atividades relacionadas a esta Política.
- Implementar esta Política.
- Promover a adoção dos elevados padrões éticos e de integridade e uma cultura forte de controle nas atividades regulares da Gestora, de modo a demonstrar a todos os Colaboradores a importância dos controles internos e o papel de cada um no processo/atividade.
- Promover o cumprimento da Lei, das regulamentações e normas internas no curso das atividades da Gestora.
- Zelar pelo desenvolvimento, pela qualidade e eficiência desta Política e dos procedimentos e controles nela estabelecidos.
- Promover a melhoria contínua dos procedimentos e controles estabelecidos nesta Política.
- Acompanhar os resultados das atividades de monitoramento de compliance, assegurando o estabelecimento de ações adequadas e em tempo razoável para a correção dos problemas e irregularidades identificados.

Diretor de Compliance e Riscos

- Desenvolver e submeter à aprovação dos Diretores esta Política.
- Elaborar, divulgar e revisar periodicamente esta Política (conforme definido neste documento).
- Disseminar a cultura de compliance e controles internos, promovendo a conscientização e enfatizando o comprometimento e engajamento de cada Colaborador na implantação das regras de compliance para garantia do sucesso desta Política.
- Alocar recursos e determinar o escopo, profundidade e frequência das atividades de compliance para alcance dos objetivos.
- Acompanhar proativamente as alterações no ambiente regulatório e as respectivas adequações dos processos em tempo hábil, de forma a assegurar o cumprimento das novas exigências regulatórias por todos os Colaboradores da Gestora.
- Monitorar o cumprimento das Leis, regulamentos, políticas internas e códigos de conduta pela Gestora e todos os Colaboradores.
- Desenvolver e aplicar testes de conformidade, sempre que necessário, para avaliar aderência com as Leis, regulamentos e normas internas.
- Assessorar no processo de desenvolvimento de novos produtos, adequada segregação de funções nas novas funções criadas ou alteradas, definindo os requisitos de segurança em conformidade com a Política de Segurança da Informação.
- Acompanhar as inspeções de órgãos reguladores, as auditorias externas e auditorias de parceiros, assegurando o pronto atendimento dos auditores, o relacionamento construtivo, e o endereçamento dos pontos de atenção e recomendações identificados nas inspeções e/ ou auditorias.
- Acompanhar e reportar aos Diretores sobre o andamento dos planos de ação que endereçam as recomendações dos órgãos reguladores, de eventual auditoria externa e de parceiros e das atividades promovidas referentes ao compliance e controles internos.
- Elaborar e encaminhar aos Diretores, sempre que necessário, um Relatório de Compliance (conforme abaixo detalhado).
- Manter os Relatórios de Compliance disponíveis para a Comissão de Valores Mobiliários na sede da Gestora.

- Manter a independência no exercício da função.
- Reportar prontamente aos Diretores qualquer situação que exponha a Gestora a risco alto ou crítico com base no Plano de Continuidade de Negócios.
- Contratar, anualmente, empresa especializada para a realização de testes de segurança e procedimentos para detectar falhas e vulnerabilidades nos sistemas da Gestora.

Colaboradores em Geral

- Cabe a todos os Colaboradores a responsabilidade por zelar pelo nome, reputação e imagem da Gestora, permitindo o crescimento perene e sustentável, e a contínua melhoria dos processos.
- Manter conduta ética compatível com os valores da Gestora, respeitando o Código de Ética e Conduta e todas as demais políticas que regem a Gestora.
- Conscientizar-se dos riscos inerentes às suas respectivas áreas de responsabilidade e de seu papel na gestão de riscos de sua área.
- Comprometer-se e engajar-se na implementação dos programas de compliance e controles internos criados pelo Diretor de Compliance e Riscos, conforme aplicável.
- Buscar o conhecimento e entendimento das principais leis, regulamentos e normativos internos que afetam sua área, avaliando os riscos e assegurando seu cumprimento.
- Reportar imediatamente a identificação de qualquer fato relevante, deficiência, falha ou não conformidade das políticas da Gestora ao seu superior hierárquico e ao Diretor de Compliance e Riscos.

2.2. REGRAS E PRINCÍPIOS NORTEADORES DAS ATIVIDADES

Definição, Aprovação e Acompanhamento - Compliance e Controles Internos

O Diretor de Compliance e Riscos é responsável por definir e submeter à aprovação dos Diretores qualquer programa de compliance, controles internos e gestão de riscos, que entender necessário, bem como pela implantação do referido programa junto aos Colaboradores da Gestora.

O Diretor de Compliance e Riscos deve elaborar um Relatório de Compliance, o qual deve ser submetido e encaminhado aos Diretores anualmente, conforme abaixo.

A execução das atividades relacionadas à gestão do compliance regulatório na Gestora deve prever os seguintes aspectos:

(a) condução periódica de processo de auto avaliação de aderência aos normativos críticos junto aos Colaboradores; e/ou
(b) desenvolvimento e aplicação de testes de conformidade independentes, sempre que necessários, para verificação do nível de aderência aos normativos internos e externos, considerando também a validação e o acompanhamento da implantação dos planos de ação estabelecidos para eventuais descumprimentos identificados.

2.3. GESTÃO DE DOCUMENTOS CORPORATIVOS

A Gestora disponibiliza a todos os seus Colaboradores as políticas internas vigentes para consulta, o que é realizado por meio do website e da intranet da Gestora, e garante que estejam sempre atualizadas.

Tais políticas internas e seus respectivos procedimentos são ferramentas de controle que auxiliam a garantir que os valores, princípios e normas da Gestora sejam definidas, divulgadas e executadas e que as respectivas ações de gerenciamento de riscos e controle do cumprimento das normas possam ser tomadas.

2.4. CONTROLES INTERNOS

A título de exemplo, citam-se os seguintes tipos de controles que podem ser implementados pela Gestora a fim de garantir o cumprimento das Leis, regulamentos e normas internas:

(a) revisão periódica pelos Diretores de tópicos que geram impacto nas estratégias da empresa para a detecção de desvios e correção dos planos propostos para o restante da empresa. Possíveis erros de controles implantados em processos também são passíveis de serem detectados neste nível;
(b) processo de revisão efetuado por um nível gerencial, com o objetivo de realizar a conferência das atividades executadas pelo nível operacional, seja por meio de um relatório sumarizado ou nas atividades diárias;
(c) verificação acerca da exatidão, integridade e autorização de transações efetuadas por meio de sistemas de informação;
(d) revisão periódica de indicadores de desempenho e a consequente detecção de desvios inesperados; e
(e) segregação de funções.

2.5. CONTROLES DE SISTEMAS DE INFORMAÇÃO E UTILIZAÇÃO DE SENHAS

O Diretor de Compliance e Riscos, além de ser responsável pelo desenvolvimento e monitoramento da Política de Segurança da Informação, incluindo a realização de avaliações de vulnerabilidades, quando aplicáveis, também é responsável por verificar a efetividade dos controles implantados em sistemas tecnológicos (controle de acesso lógico, segurança de banco de dados etc.).

A utilização de senhas para acesso às estações de trabalho, correios eletrônicos (e-mails), software e demais dispositivos que se façam necessários é obrigatória, cabendo a cada Colaborador a responsabilidade pelo respectivo resguardo e confidencialidade, não as repassando a terceiros. As senhas deverão possuir validade máxima de 1 (um) ano e podem ser substituídas a qualquer momento por decisão do Diretor de Compliance e Riscos ou por solicitação formal do Colaborador.

Todos os Colaboradores estão cientes de que toda informação gerada internamente pela Gestora e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência. Além disso, os Colaboradores, ao utilizarem qualquer meio eletrônico (chats, Skype, e-mails, internet, entre outros) para o desenvolvimento de suas atividades, devem considerar seu uso como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os

acessos a e-mails e à internet, assim entendidos como ferramentas de trabalho de propriedade da Gestora, são armazenados de forma segura em nossa solução em nuvem, utilizando criptografia e outras medidas de segurança, são gerenciados pelo Diretor de Compliance e Riscos da Gestora que aplica e monitora os requisitos de acesso, e poderão ser objeto de auditorias e revisões a qualquer momento, estando à total disposição da administração da empresa.

A responsabilidade do Colaborador e/ou prestador de serviços em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os itens desta Política.

O Colaborador está ciente de que o não cumprimento das disposições acima previstas e dos demais termos desta Política será considerado infração grave, passível de advertência formal e sujeito à imposição de sanções administrativas, as quais, em casos extremos, incluem o desligamento do profissional embasado em legislação vigente, trabalhista ou não. Eventuais violações às disposições previstas nesta Política serão tratadas de maneira individual e levadas imediatamente à avaliação do Diretor de Compliance e Riscos da Gestora.

Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a Gestora cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para fins pessoais. Adicionalmente, a Gestora recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da internet, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis, conforme parágrafo anterior.

Com o objetivo de garantir maior alinhamento da conduta de todos os seus Colaboradores, este documento abordará alguns itens de maneira direta e específica. Vale salientar, entretanto, que esta Política não deve se restringir aos aspectos tratados a seguir e que eventuais dúvidas e/ou questionamentos devem ser imediatamente levados ao conhecimento do Diretor de Compliance e Riscos da Gestora.

3. UTILIZAÇÃO DE SENHAS

A utilização de senhas para acesso às estações de trabalho, correios eletrônicos (e-mails), software e demais dispositivos que se façam necessários é obrigatória, cabendo a cada Colaborador a responsabilidade pelo respectivo resguardo e confidencialidade, não as repassando a terceiros. As senhas deverão possuir validade máxima de 1 (um) ano e podem ser substituídas a qualquer momento por decisão do Diretor de Compliance e Riscos ou por solicitação formal do Colaborador.

4. UTILIZAÇÃO DA INTERNET

Como já explorado anteriormente, a utilização da internet no ambiente da Gestora deve restringir-se a assuntos profissionais. Ainda assim, a Gestora solicita a cada um de seus Colaboradores que empregue os mais elevados padrões éticos para a utilização deste meio e define as seguintes diretrizes para sua utilização:

(a) a internet não pode ser utilizada como ferramenta para download ou distribuição de software ou dados não legalizados, acesso a páginas de jogos, material pornográfico, sites de compras, sites de relacionamento, entre outros de conteúdo impróprio;

(b) a internet não deve ser utilizada como ferramenta para a divulgação de informações confidenciais em grupos de discussão, Instant Messenger ou "salas de bate papo", não importando se a divulgação foi deliberada ou inadvertida;

(c) caso a Gestora julgue necessário, haverá bloqueios de acesso a arquivos e/ou domínios que possam comprometer o uso de banda ou que impactem o bom andamento dos trabalhos;

(d) a Gestora possui controle de todo conteúdo considerado confidencial acessado pelos Colaboradores;

(e) o acesso à internet deve, obrigatoriamente, ser realizado por meio do programa Internet Explorer, ou Google Chrome, ou outro software desde que devidamente homologado pelo Diretor de Compliance e Riscos da Gestora; e

(f) as áreas de armazenamento da Gestora no sistema Onedrive com acesso exclusivo para os colaboradores da Gestora e onde não devem ser utilizadas para arquivamento de itens de natureza pessoal.

5. UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

É proibida a utilização do correio eletrônico para:

(a) envio de mensagens ofensivas, difamatórias, preconceituosas, ou que possam causar hostilidade de qualquer espécie (de conteúdo religioso, sexual, político ou racial), ou que comprometam a imagem da Gestora;

(b) envio de mensagens por outros usuários que não os responsáveis pelo login e pela senha de acesso ao sistema;

(c) envio de mensagens que solicitem inscrição em listas de distribuições de mensagens na internet de assuntos não relacionados aos negócios da Gestora;

(d) envio de mensagens com o objetivo de prejudicar o serviço de indivíduos e/ou empresas (quantidade ou tamanho excessivo de mensagens, código malicioso etc.);

(e) envio de mensagens que levem o destinatário a incorrer em erro de identificação do emitente (se passar por outra pessoa);

(f) envio de mensagens cujo objetivo seja a venda de serviços e/ou produtos não relacionados aos negócios da Gestora;

(g) envio de mensagens, cujo conteúdo seja confidencial ou restrito à Gestora e não possa se tornar público;

(h) execução de arquivos anexados a mensagens recebidas de emitentes desconhecidos ou suspeitos;

(i) prática de ato que, de qualquer forma, possa ferir a legislação em vigor, as regras de sigilo bancário e direitos autorais;

(j) prática de ato em contraste com os deveres profissionais e com os interesses da Gestora, ou a fim de violar esta Política;

(k) recebimento de arquivos do tipo vídeo (*.avi, *.mpeg, entre outros).

(l) o recebimento de arquivos do tipo "executáveis" (programas) será controlado por programa antivírus contido nos equipamentos de controle de mensagens; e

(m) a assinatura de e-mail será atribuída de forma automática (não é necessário assinar durante a composição da mensagem) e seguirá o seguinte padrão:

[Nome do Funcionário]
[Cargo]
[Logo da gestora]
[Telefone]
[E-mail]
[Site da gestora]
[Endereço da gestora]
[Disclaimer relativo à confidencialidade das informações, devidamente aprovado pelo Diretor de Compliance e Riscos].]

6. UTILIZAÇÃO DE SOFTWARE

Tendo em vista que os equipamentos de informática disponibilizados pela Gestora se destinam ao desempenho de atividades profissionais, a utilização de software e a instalação de arquivos executáveis e/ou aplicativos que tenham potencial de exposição de informações confidenciais nas estações de trabalho ou na rede da Gestora é terminantemente proibida, exceto em casos em que haja avaliação, controles e testes de segurança, e expressa autorização por parte do Diretor de Compliance e Riscos.

7. ACESSO A SISTEMAS, BASES DE DADOS E REDES

O acesso a sistemas, bases de dados e redes é restrito e definido em função do perfil de cada Colaborador da Gestora. O detalhamento do perfil de acesso de cada Colaborador (incluindo operadores e eventuais prestadores de serviços) é realizado no momento da contratação e criteriosamente analisado pelo Diretor de Compliance e Riscos para cada caso. A liberação do acesso a qualquer sistema, base de dados ou endereço de rede depende de prévia aprovação do Diretor de Compliance e Riscos.

Diante do exposto acima, ficam aqui estabelecidas as seguintes diretrizes:

(a) tentativas para obtenção de acesso não autorizado (fraude de autenticação de usuário ou segurança de qualquer servidor, rede ou conta) não são permitidas. Inclui-se neste

ponto o acesso a dados não disponíveis para o usuário, bem como a tentativa de conexão a servidores ou contas cujo acesso não tenha sido expressamente autorizado e situações que coloquem à prova a segurança de outras redes;

(b) tentativas de interferência nos serviços de qualquer outro usuário, servidor ou rede não são permitidas. Inclui-se neste ponto ataques do tipo "negativa de acesso", congestionamento em redes, bem como tentativas deliberadas de sobrecarga e/ou invasão de um servidor;

(c) materiais de conteúdo inapropriado (ex.: pornografia) não podem ser expostos, armazenados, distribuídos, editados ou gravados por meio do uso dos recursos computacionais da rede;

(d) a pasta TRANSFERÊNCIA (ou similar) não deverá ser utilizada para armazenamento de arquivos que contenham materiais de natureza sigilosa ou sensível;

(e) a armazenagem de arquivos inerentes às atividades profissionais desempenhadas por cada um dos Colaboradores da Gestpra nos servidores de arquivos é obrigatória. Tal medida visa assegurar a realização de backups de segurança; e

(f) a varredura simples ou em massa, visando a descoberta de endereços ou portas e/ou qualquer ataque ou tentativa de invasão é terminantemente proibida.

8. UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho destinam-se exclusivamente ao exercício e ao desempenho de atividades profissionais por cada um dos Colaboradores da Gestora. A responsabilidade pela manutenção da integridade física das estações de trabalho cabe a cada um dos Colaboradores da empresa, sendo vedada a realização de qualquer alteração em termos de configuração, sem prévio consentimento por escrito do Diretor de Compliance e Riscos. Da mesma forma, cabe a cada um dos Colaboradores bloquear a respectiva estação de trabalho virtual durante período de ausência, de forma a garantir a total confidencialidade e integridade das informações manipuladas por este.

Cada Colaborador deve manter sua mesa de trabalho limpa e organizada, não deixando papéis de trabalho, relatórios ou qualquer documento confidencial em cima da mesa. Isso também é valido para scanner e impressora, ao utilizar os equipamentos, os documentos escaneados e impressos devem ser retirados imediatamente.

9. UTILIZAÇÃO DE MENSAGEIROS ELETRÔNICOS

Conforme informações apresentadas anteriormente, todo e qualquer dispositivo de mensagens eletrônicas deve ser encarado como ferramenta de trabalho e, como tanto, é de propriedade da empresa e destina-se a assuntos profissionais e de interesse da organização. Por se tratar de ferramenta de trabalho, todos os dispositivos estão sujeitos aos mecanismos de controle impostos pela Gestora e terão os respectivos históricos gravados e devidamente arquivados para utilização em caso de necessidades.

Seguindo a mesma linha de atuação imposta aos demais requerimentos definidos por meio desta Política, a utilização de dispositivos de mensagens eletrônicas sem a devida aprovação e liberação por parte do Diretor de Compliance e Riscos e/ou a utilização das ferramentas disponibilizadas pela Gestora para a tratativa de assuntos pessoais serão alvo de constante fiscalização e poderão implicar em penalidades aos envolvidos, conforme definição estabelecida pelo Diretor de Compliance e Riscos.

10. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Como forma de preservar informações confidenciais detidas pela Gestora, seguimos ainda as medidas de segurança abaixo:

(a) Sistema de Armazenamento de Dados. A Gestora adota o sistema de servidores remotos da Microsoft (Onedrive) para gerenciar suas informações. Nesse sistema, os arquivos eletrônicos ficam armazenados remotamente em servidores seguros e com redundância. Por meio desse sistema, somente usuários com senha conseguem acessar as informações confidenciais, evitando que pessoas não autorizadas tenham acesso a tais informações. O acesso é feito com uso de senhas pessoais e intransferíveis, com procedimento de verificação em 2 (duas) etapas (login e senha) e por meio de equipamento (computador, celular, tablet) previamente cadastrado e aprovado. Qualquer atividade na rede é monitorada, identificada (usuário, computador e IP que acessou o sistema), e pode ser revertida ou bloqueada. O sistema possui, ainda, diferentes níveis de acesso aos arquivos, sendo possível realizar restrições de nível de pasta e arquivo o que garante maior confidencialidade das informações e redução do risco de uso indevido dessas. Por fim, o sistema realiza um backup diário das informações armazenadas localmente e redundância no armazenamento das informações e arquivos nos servidores remotos, de modo que na ocorrência de problemas como perda de dados, os arquivos e as informações podem ser recuperados rapidamente dos servidores remotos sem grandes interrupções nas atividades da equipe.

(b) Trituração de Material Confidencial. Documentos considerados sensíveis são triturados previamente ao seu descarte, evitando assim o acesso fraudulento a nossas informações.

(c) Segregação de Informações Decorrentes de Atividades Distintas. A segregação das informações é realizada por meio de restrições ao acesso às informações de um departamento por Colaboradores de outro. Cada departamento possui um diretório próprio de armazenamento de documentos, o qual é acessado por meio de senhas e *logins* individuais.

(d) Testes de Segurança: A contratação, periodicamente, de testes de segurança e procedimentos para detectar falhas e vulnerabilidades nos sistemas da Gestora, bem como para viabilizar a identificação dos detentores de informações confidenciais e privilegiadas para responsabilização, em caso de vazamento.

Em caso de ocorrência de vazamento de dados e informações confidenciais, reservadas ou privilegiadas, seja em caso de identificação durante atividades de monitoramento ou se vier ao

conhecimento da Gestora por qualquer meio, a Gestora, por meio do seu Diretor de Compliance e Riscos, adotará todas as medidas necessárias para atender a demandas de órgãos reguladores e da lei, levando em conta as diretrizes previstas na respectiva política. Ainda, o Diretor de Compliance e Riscos deverá avaliar a necessidade de comunicação aos clientes, tendo em vista as determinações legais e regulamentares.

A comunicação com órgãos e entidades governamentais é pautada pelas seguintes diretrizes:
(a) os documentos e relatórios produzidos pelo Diretor de Compliance e Riscos, quando previstos em legislação específica, devem ficar à disposição de órgãos reguladores;
(b) ao serem solicitados, estes documentos devem passar por um processo de revisão e autorização de envio, tanto do Diretor de Compliance e Riscos, quanto dos Diretores;
(c) o atendimento aos ciclos de inspeção dos órgãos reguladores deve ser coordenado pelo Diretor de Compliance e Riscos e todos devem ser orientados a dar prioridade máxima ao atendimento das demandas originadas nestes ciclos de inspeção; e
(d) o resultado das auditorias ou inspeções deve gerar um plano de ação para atendimento às exigências, cujo follow-up de atividades junto aos Colaboradores deve ficar a cargo do Diretor de Compliance e Riscos.

11. CLASSIFICAÇÃO DAS INFORMAÇÕES

A fim de determinar o nível de proteção e garantir a segurança do compartilhamento de informações, a Gestora classifica as informações que transitam em seu ambiente físico e eletrônico da seguinte maneira: (a) pública - informação sobre a qual não há restrições quanto à divulgação, acessível a qualquer pessoa sem causar quaisquer consequências danosas aos processos da empresa; (b) interna - informação que a organização não tem interesse de divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso esta informação seja disponibilizada, não haverá danos sérios à empresa; e (c) confidencial - informação interna da organização, cuja divulgação pode causar danos financeiros ou à imagem da empresa. A divulgação ainda pode gerar vantagens a eventuais concorrentes e perda de clientes.

11.1. ATENDIMENTO A ÓRGÃOS REGULADORES, AUDITORES EXTERNOS E TERCEIROS

O atendimento a demandas de órgãos reguladores é prioritário, sobrepondo-se às atividades cotidianas do Diretor de Compliance e Riscos.

A comunicação com tais órgãos é pautada pelas seguintes diretrizes:

- **(a)** os documentos e relatórios produzidos pelo Diretor de Compliance e Riscos, quando previstos em legislação específica, devem ficar à disposição de órgãos reguladores;
- **(b)** ao serem solicitados, estes documentos devem passar por um processo de revisão e autorização de envio, tanto do Diretor de Compliance e Riscos, quanto dos Diretores;
- **(c)** o atendimento aos ciclos de inspeção dos órgãos reguladores deve ser coordenado pelo Diretor de Compliance e Riscos e todos devem ser orientados a dar prioridade máxima ao atendimento das demandas originadas nestes ciclos de inspeção; e

(d) o resultado das auditorias ou inspeções deve gerar um plano de ação para atendimento às exigências, cujo *follow-up* de atividades junto aos Colaboradores deve ficar a cargo do Diretor de Compliance e Riscos.

11.2. RELATÓRIO DE COMPLIANCE

O Relatório de Compliance, a ser apresentado aos Diretores, até o último dia útil do mês de abril de cada ano, nos termos do art. 25, da Resolução 21 de 25 de fevereiro de 2021 e alterações posteriores, deverá basear-se no acompanhamento sistemático das atividades relacionadas com o sistema de controles internos da Gestora, conforme determinado na legislação aplicável, e deverá conter:

(a) as conclusões dos exames efetuados;
(b) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento destas, quando for o caso; e
(c) a manifestação do Diretor de Gestão de Recursos, ou quando for o caso, do Diretor de Compliance e Riscos, a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

Os Relatórios de Compliance deverão ser mantidos à disposição da Comissão de Valores Mobiliários na sede da Gestora.

12. TREINAMENTOS E CAPACITAÇÃO DE COMPLIANCE

O Diretor de Compliance e Riscos é responsável pelo desenvolvimento de planos de treinamento, capacitação e conscientização, com a periodicidade que entender necessária considerando a alteração das políticas da Gestora e/ou a rotação de Colaboradores, em assuntos relacionados às atividades de compliance e controles internos, necessários para o fortalecimento da cultura de compliance interno de todos os Colaboradores da Gestora.

Dentre outros assuntos a serem propostos, os treinamentos devem ser previstos para os seguintes assuntos:

(a) Código de Ética e Conduta;
(b) Política de Segurança da Informação;
(c) Política de Conheça seu Cliente e Prevenção e Combate à Lavagem de Dinheiro e Financiamento ao Terrorismo; e
(d) Política de Continuidade de Negócios.

Todos os treinamentos poderão ser realizados de modo presencial ou online e a participação dos Colaboradores de todos os níveis hierárquicos da Gestora será obrigatória.

13. PLANO DE CONTINUIDADE DE NEGÓCIOS

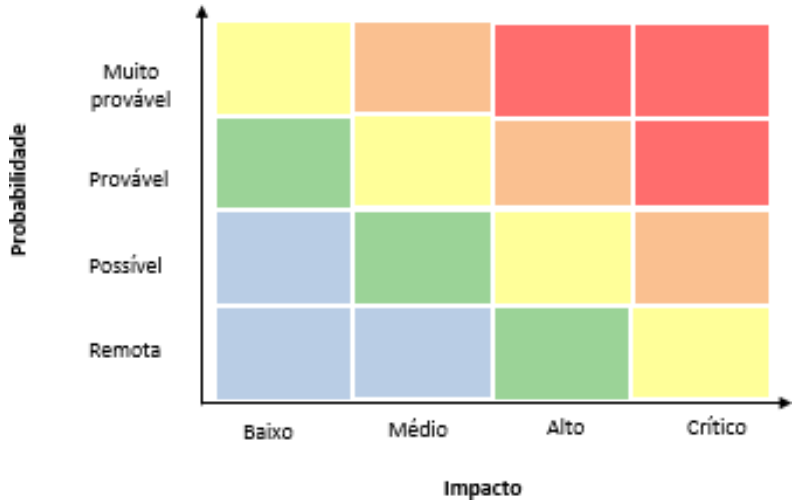
13.1. GESTÃO, ATUALIZAÇÃO E DIVULGAÇÃO

O Plano de Continuidade de Negócios ("PCN") foi elaborado levando em consideração os negócios desenvolvidos pela Gestora e suas implicações e tem como objetivo minimizar os efeitos de acontecimentos de naturezas variadas, que possam prejudicar parcial ou totalmente o desenvolvimento dos negócios da Gestora.

A atualização e a divulgação do PCN serão realizadas pelo Diretor de Compliance e Riscos a qualquer momento, desde que sejam identificadas melhorias ou alterações nos procedimentos que compõem o PCN. A divulgação do PCN será feita no drive da Gestora e em material impresso.

13.2. CENÁRIOS DE RISCOS E POTENCIAL IMPACTO NA OPERAÇÃO

Os cenários de riscos e o potencial impacto na operação da Gestora são avaliados de acordo com o impacto e com a probabilidade de ocorrência dos eventos associados aos fatores de riscos. O resultado da avaliação de riscos auxilia na tomada de decisões acerca da prioridade para tratamento dos riscos identificados, de modo que riscos com baixo impacto e baixa probabilidade possuem menor prioridade de tratamento do que os riscos com alto impacto e alta probabilidade de ocorrência, conforme demonstrado no fluxograma a seguir:



13.3. MANUTENÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

O Diretor de Compliance e Riscos da Gestora deverá elaborar um relatório, conforme aplicável, sobre os eventuais riscos apresentados que possam impactar a continuidade dos negócios da Gestora, bem como propor soluções para eliminar, diminuir ou transferir o evento de risco (ex. com a contratação de seguros). Poderá, ainda, se entender necessário, implementar atividades de manutenção do PCN.

13.4. PROCEDIMENTO DE ATIVAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS ("PLANO DE CONTINGÊNCIA")

O cenário definido como crítico é a indisponibilidade de acesso às dependências internas da Gestora, bem como a indisponibilidade dos equipamentos que suportam a operação. Neste contexto, será acionado o Plano de Contingência pelo Diretor de Compliance e Riscos da Gestora ou, em sua ausência, por qualquer membro da administração/diretoria da Gestora. A empresa utiliza o serviço de

armazenamento em nuvem do Microsoft (Onedrive) e suas devidas rotinas de segurança e backup, bem como serviço de e-mail prestado pela Microsoft - Outlook e suas devidas rotinas de segurança e backup. e todas as operações realizadas pelos Colaboradores da Gestora serão via acesso remoto em ambiente externo a ser determinado oportunamente.

O Diretor de Compliance e Riscos da Gestora terá a responsabilidade de comunicar os clientes da impossibilidade da Gestora em operar em condições normais, informando que a Gestora estará em contingência buscando manter as atividades, embora com capacidade reduzida de recursos.

Em caso de problemas para locomoção das pessoas envolvidas no Plano de Contingência, a Gestora será responsável pelo transporte e custos envolvidos. Como alternativa, poderão ser configurados equipamentos com acesso remoto para os Colaboradores, sob gestão do Diretor de Compliance e Riscos da Gestora. Assim, no caso de uma ocorrência que interrompa o uso da infraestrutura da Gestora de forma temporária ou permanente, devem ser tomadas as seguintes medidas dependendo das circunstâncias específicas:

- Recuperação do backup dos dados armazenados em nuvem instantaneamente para possibilitar a continuidade de análises, geração de informações e comunicação com cotistas e empresas-alvo investidas.

- Disponibilização de notebooks ou recursos de processamento para pessoas chave de modo a restaurar o quanto antes o fluxo de análises, relatórios e informações dentro e fora da empresa (principais executivos já possuem notebook, ou seja, capacidade de processamento remota; a aquisição de novos computadores, caso necessário, pode ser viabilizada em 24-48 horas).

- Caso necessário, o uso de um local remoto como escritório temporário para contornar problemas específicos que venham a ocorrer na sede da empresa. As operações serão automaticamente migradas para a sede principal da Gestora tão logo as instalações estiverem aptas para o desenvolvimento normal dos negócios.

Sem prejuízo do disposto acima, a Gestora conta ainda com potenciais prestadores de serviços externos para sistema de acompanhamento de investimentos e gestão de riscos (Comdinheiro), administração fiduciária focada em FIDCs, FIPs e FIFs, além de software de suporte para gestão operacional (Kanastra), os quais, caso haja demanda operacional, poderão ser contratados pela Gestora prontamente.

13.5. CONFIDENCIALIDADE E DEMAIS TERMOS GERAIS

A presente Política tem como objetivo central apresentar e disseminar entre todos os Colaboradores da Gestora as políticas e os procedimentos definidos pelo Diretor de Compliance e Riscos para garantir a integridade das informações produzidas e gerenciadas dentro do ambiente de trabalho.

A Gestora estabelece que é responsabilidade de cada um de seus Colaboradores garantir a total confidencialidade e integridade das informações diariamente produzidas em razão de e/ou no ambiente de trabalho, sendo essencial que todo Colaborador tenha plena consciência acerca de sua

importância no processo de garantia do cumprimento dos procedimentos definidos por meio desta Política.

Os Colaboradores deverão observar as regras de sigilo e conduta adotadas pela Gestora, incluindo, sem limitação, para os detentores de informações privilegiadas em função de seu cargo ou atribuição, de forma a estabelecer uma barreira de informações com os demais Colaboradores.

Todos os Colaboradores estão cientes de que toda informação gerada internamente pela Gestora e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência. Além disso, os Colaboradores, ao utilizarem qualquer meio eletrônico (chats, ferramentas de conferência, e-mails, internet, entre outros) para o desenvolvimento de suas atividades, devem considerar seu uso como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os acessos a e-mails e à internet, assim entendidos como ferramentas de trabalho de propriedade da Gestora, passam por backups diários e poderão ser objeto de auditorias e revisões a qualquer momento, estando à total disposição da administração da empresa.

A responsabilidade do Colaborador em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os itens desta Política.

O Colaborador está ciente de que o não cumprimento das disposições acima previstas e dos demais termos desta Política será considerado infração grave, passível de advertência formal e sujeito à imposição de sanções administrativas, as quais, em casos extremos, incluem o desligamento do profissional embasado em legislação vigente, trabalhista ou não. Eventuais violações às disposições previstas nesta Política serão tratadas de maneira individual e levadas imediatamente à avaliação do Diretor de Compliance e Riscos da Gestora.

Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a Gestora cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para fins pessoais. Adicionalmente, a Gestora recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da internet, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis, conforme parágrafo anterior.

Com o objetivo de garantir maior alinhamento da conduta de todos os seus Colaboradores, este documento abordará alguns itens de maneira direta e específica. Vale salientar, entretanto, que esta Política não deve se restringir aos aspectos tratados a seguir e que eventuais dúvidas e/ou questionamentos devem ser imediatamente levados ao conhecimento do Diretor de Compliance e Riscos da Gestora.

A presente Política deverá passar por processo de revisão, ao menos, a cada 2 (dois) anos pelo Diretor de Compliance e Riscos. Eventuais alterações serão prontamente comunicadas a todos os Colaboradores da Gestora e disponibilizadas no website deste. Os Colaboradores deverão assinar termo de compromisso de cumprimento das obrigações de confidencialidade aqui previstas, bem como das demais políticas e códigos da Gestora.

Eventuais dúvidas ou questionamentos devem ser diretamente encaminhados ao Diretor de Compliance e Riscos conforme abaixo:

Nome: Luis Otavio Rodeguero
E-mail: luis.rodeguero@kortexventures.com
Endereço: Rua Viradouro, 63 – Conjunto 71 – Itaim Bibi – São Paulo - SP

MODELO DE TERMO DE COMPROMISSO DE CONFIDENCIALIDADE E ADESÃO ÀS POLÍTICAS DA GESTORA KX VENTURES LTDA.

("TERMO DE ADESÃO E COMPROMISSO")

[**Nome e qualificação do aderente**] ("Aderente"), por meio do presente Termo de Compromisso de Confidencialidade e Adesão às Políticas e Código de Ética da **KX VENTURES Ltda.**, com sede em São Paulo, Estado de São Paulo, na Rua Francisco Leitão, 104, apto. 63, Pinheiros, São Paulo/SP, CEP 05414-020, inscrita no CNPJ/MF sob o nº 53.069.721/0001-14 ("Sociedade" ou "Gestora"), com seus atos constitutivos arquivados na Junta Comercial do Estado de São Paulo ("JUCESP") sob o NIRE 35.262.697.024 declara ter conhecimento e ter recebido cópia de tais políticas e códigos, incluindo a Política de Confidencialidade, Segurança da Informação e Programa de Treinamento e o Código de Ética da Sociedade ("Códigos e Políticas"), e aceita os respectivos termos:

1. ADESÃO ÀS POLÍTICAS

1.1. Tendo em vista o vínculo do Aderente com a Sociedade, o Aderente neste ato declara ter conhecimento e ter recebido todas as informações e orientações para cumprimento das disposições dos Códigos e Políticas, incluindo, sem limitação, a Política de Regras, Procedimentos e Controles Internos, assim como os devidos treinamentos para, além de estar ciente de todos os termos e condições, concordar e reconhecer que estará sujeito às disposições, direitos e obrigações aplicáveis nos termos dos Códigos e Políticas, sendo certo que os direitos e obrigações previstos em referidos Códigos e Políticas vinculam o Aderente desde o início de seu vínculo com a Sociedade.

1.2. A Aderente declara que revisou integralmente os Códigos e Políticas e que tem pleno conhecimento de seus termos e condições, bem como que se obriga a realizar, cumprir e a fazer com que seus representantes realizem e cumpram todos os direitos e obrigações decorrentes dos Códigos e Políticas.

2. CONFIDENCIALIDADE

2.1. A Aderente obriga-se a guardar o mais completo sigilo por si, por seus empregados ou prepostos, nos termos da Lei Complementar nº 105, de 10 de janeiro de 2001, que trata do sigilo das operações de instituições financeiras, e da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – "LGPD"), cujo teor declara ser de seu inteiro conhecimento, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venha(m) tomar conhecimento

ou ter acesso, em razão de sua atuação na Sociedade, ficando, na forma da lei, responsável pelas consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei.

2.2. O Aderente reconhece e concorda que é sua responsabilidade e de cada um de seus representantes garantir a total confidencialidade e integridade das informações diariamente produzidas em razão de e/ou no ambiente de trabalho, sendo essencial que todo colaborador tenha plena consciência acerca de sua importância no processo de garantia do cumprimento dos procedimentos definidos por meio dos Códigos e Políticas.

2.3. O Aderente desde já se obriga a observar as regras de sigilo e conduta adotadas pela Gestora, incluindo, sem limitação, para os detentores de informações privilegiadas em função de seu cargo ou atribuição, de forma a estabelecer uma barreira de informações com os demais colaboradores da Sociedade.

2.4. O Aderente está ciente e concorda, obrigando-se a manter sigilo, que toda informação gerada internamente pela Gestora e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência. Além disso, o Aderente, e qualquer de seus representantes, ao utilizarem qualquer meio eletrônico (chats, ferramentas de conferência, e-mails, internet, entre outros) para o desenvolvimento de suas atividades, devem considerar seu uso como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os acessos a e-mails e à internet, assim entendidos como ferramentas de trabalho de propriedade da Gestora, passam por backups diários e poderão ser objeto de auditorias e revisões a qualquer momento, estando à total disposição da administração da empresa.

2.5. A responsabilidade do Aderente em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os Códigos e Políticas.

2.6. O Colaborador está ciente de que o não cumprimento das disposições acima previstas e dos demais termos deste instrumento e/ou dos Códigos e Políticas será considerado infração grave, passível de advertência formal e sujeito à imposição de sanções administrativas, as quais, em casos extremos, incluem o desligamento do profissional embasado em legislação vigente, trabalhista ou não. Eventuais violações às disposições previstas neste instrumento

e/ou nos Códigos e Políticas serão tratadas de maneira individual e levadas imediatamente à avaliação do Diretor de Compliance e Riscos da Gestora.

2.7. Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a Gestora cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para fins pessoais. Adicionalmente, a Gestora recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da internet, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis, conforme item anterior.

2.8. O Aderente declara que leu e entendeu todos os termos, condições, tem ciência e concorda em observar os termos dos Códigos e Políticas, declarando, ainda, o quanto segue: (i) possui plena capacidade, poder e autoridade e obteve todas as aprovações requeridas para (a) executar, assinar e entregar o presente Termo de Adesão e qualquer acordo ou instrumento referido ou contemplado por este Termo de Adesão; e (b) cumprir integralmente todas as obrigações contempladas neste Termo de Adesão ou nos documentos relacionados; (ii) a assinatura, entrega e execução do presente Termo de Adesão não (a) requer nenhum consentimento ou aprovação que não foi obtida; (b) viola qualquer lei, decreto, regulamento ou ordem de uma autoridade competente que esteja em vigor na presente data; ou (c) viola qualquer acordo, documento ou outro instrumento firmado em benefício de ou com qualquer terceiro; (d) não violou nem determinou que quaisquer administradores, gerentes, empregados, prestadores de serviços e/ou quaisquer pessoas agindo em seus nomes, direta ou indiretamente, violassem as disposições das leis anticorrupção aplicáveis.

2.9. Este Termo de Adesão constitui título executivo extrajudicial, nos termos do Código de Processo Civil Brasileiro. O presente Termo de Adesão será regido e interpretado de acordo com as leis da República Federativa do Brasil. Como parte integrante do Contrato, este Termo de Adesão seguirá as regras de resolução de conflitos estipuladas no Contrato.

EM TESTEMUNHO DE QUE, o(s) signatário(s) deste Termo de Adesão, assinado eletronicamente por meio de plataforma (i.e. DocuSign, ClickSign etc.), pelo que as Partes expressamente declaram, de maneira inequívoca, que tal modalidade de assinatura é juridicamente válida, exequível e suficiente para vincular as Partes a todos os termos e condições deste Termo de Adesão. Além disso, as Partes reconhecem que os documentos em formato eletrônico são plenamente válidos (como se em formato físico estivessem) e declaram que são de fato os assinantes do Termo de Adesão, nos termos do artigo 10,

Parágrafo 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, e do artigo 6º, do Decreto nº 10.278/2020. As Partes renunciam à possibilidade de exigir a troca, envio ou entrega das vias originais (não-eletrônicas) assinadas deste Termo de Adesão, bem como renunciam ao direito de recusar ou contestar a validade das assinaturas eletrônicas, na medida máxima permitida pela legislação aplicável. Ainda que alguma das Partes venha a assinar digitalmente este Termo de Adesão em local diverso, o local de celebração deste Termo de Adesão é, para todos os fins, a cidade de São Paulo, Estado de São Paulo, conforme abaixo indicado. Ademais, será considerada a data de assinatura deste Termo de Adesão, para todos os fins e efeitos, a data em que a última das assinaturas digitais for realizada, não obstante a data de assinatura indicada abaixo. Conforme aplicável, os signatários deste Termo de Adesão que o assinaram por meio de certificado digital declaram que estão e sempre estiveram em posse de seu certificado digital e que não o transferiram ou deram acesso ao seu certificado digital a qualquer terceiro, bem como realizaram pessoalmente o procedimento de validação da assinatura digital deste Termo de Adesão na plataforma.

[local e data]

[**ADERENTE**]

Testemunhas:

_____ _____

Nome: Nome:

RG: RG: