POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DA

LIGHTROCK GESTORA DE RECURSOS LTDA.

23 DE MARÇO DE 2021

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÂO

1.1. INTRODUÇÃO

LIGHTROCK GESTORA DE RECURSOS LTDA., é uma sociedade empresária limitada com sede no município de São Paulo, estado de São Paulo, na Rua Joaquim Floriano, nº 1120, conjunto 122, CEP 04.534-004, inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Economia ("CNPJ/ME") sob nº 27.927.837/0001-37 ("Gestora"), credenciada pela Comissão de Valores Mobiliários ("CVM") para o exercício profissional da atividade de administração de carteira de valores mobiliários, na categoria de gestor de recursos, nos termos da Instrução da CVM nº 558, de 26 de março de 2015 ("ICVM 558/15").

A Gestora é integrante do grupo Lightrock ("Grupo Lightrock"), um grupo global de gestão de ativos e valores mobiliários, que atua como gestor de fundos de investimento especializados e outros veículos de investimento, que investem em uma vasta gama de setores, localidades geográficas, classes de ativos e estratégias de investimento.

Em vista da natureza das atividades de gestão que desenvolve, a Gestora está sujeita a extensa legislação, regulamentação e autorregulação no mercado brasileiro. A fim de atender integralmente às exigências da legislação, regulamentação e autorregulação aplicáveis, bem como adaptar as suas atividades às melhores práticas de mercado, a Gestora adota as seguintes políticas internas: (i) código de ética e conduta; (ii) política de negociação de valores mobiliários; (iii) política de gestão de riscos; (iv) plano de negócios; (v) esta Política de Segurança da Informação (conforme abaixo definida); (vi) política de divisão e rateio de ordens; (vii) política de *compliance* e controles internos; e (viii) política de prevenção à lavagem de dinheiro e ao financiamento ao terrorismo ("PLDFT) (conjuntamente, as "Políticas Internas").

Todos os sócios, diretores, administradores e empregados da Gestora diretamente envolvidos com as atividades de administração de carteira de valores mobiliários ("Colaboradores"), vinculados à Gestora na data de elaboração das Políticas Internas e/ou que venham a integrar o corpo de profissionais da Gestora futuramente deverão receber uma via (em versões impressa e digitalizada) das Políticas Internas.

A Gestora estabelece a presente política de segurança da informação ("Política de Segurança da Informação"), com o intuito de estabelecer os princípios, conceitos e valores que deverão pautar a segurança da informação da Gestora na sua atuação interna e com o mercado, assim como suas relações com os diversos públicos.

O seu objetivo é assegurar que as informações da organização estão sendo tratadas de forma adequada para a garantia dos critérios de Confidencialidade, Integridade e Disponibilidade, conforme abaixo definidos.

Além disso, descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Os princípios e regras desta Política de Segurança da Informação devem ser observados por todos os Colaboradores da Gestora.

Ao receberem uma via da presente Política de Segurança da Informação, os Colaboradores deverão firmar termo de adesão, conforme o modelo constante no Anexo I da Política de *Compliance* e Controles Internos da Gestora ("Termo de Adesão").

Os Colaboradores também poderão consultar a presente Política de Segurança da Informação no endereço eletrônico da Gestora: www.lightrock.com.

A presente Política de Segurança da Informação deverá ser atualizada a cada três anos, no mínimo, pelo Diretor de *Compliance*, Risco e PLDFT da Gestora, a fim de contemplar as eventuais alterações da legislação, regulamentação, autorregulação e melhores práticas aplicáveis. Sempre que a presente Política de Segurança da Informação for atualizada, os Colaboradores deverão receber uma nova via da Política de Segurança da Informação atualizada (impressa e digitalizada), devendo firmar novo Termo de Adesão.

Os Termos de Adesão firmados por Colaboradores serão digitalizados e arquivados pelo Diretor de *Compliance*, Risco e PLDFT, devendo ser mantidos durante todo o prazo de relacionamento profissional com o Colaborador e por período adicional de, no mínimo, 5 (cinco) anos contados da data de desligamento do Colaborador, por qualquer motivo.

Em complementação à leitura desta Política de Segurança da Informação, todos os Colaboradores deverão ler e entender o conjunto de normas aplicáveis à Gestora no âmbito legal, regulamentar e de autorregulação. Em caso de dúvidas acerca das normas a serem analisadas e/ou quanto à interpretação do conteúdo destas normas, os Colaboradores deverão contatar o Diretor de *Compliance*, Risco e PLDFT para os devidos esclarecimentos.

As disposições da Política de Segurança da Informação deverão ser interpretadas de forma integrada pelos Colaboradores, os quais deverão levar em consideração o conjunto de políticas internas da Gestora, bem como a legislação, regulamentação, autorregulação e melhores práticas de mercado aplicáveis.

Estrutura Organizacional da Gestora

A Gestora foi criada para atuar na gestão de carteira de valores mobiliários e sua estrutura organizacional é dividida em 2 (duas) áreas distintas, a saber: (i) gestão de recursos, e (ii) *compliance*, gestão de riscos e PLDFT. A Gestora estabelece e desenvolve mecanismos para garantir a atuação independente de todas as áreas.

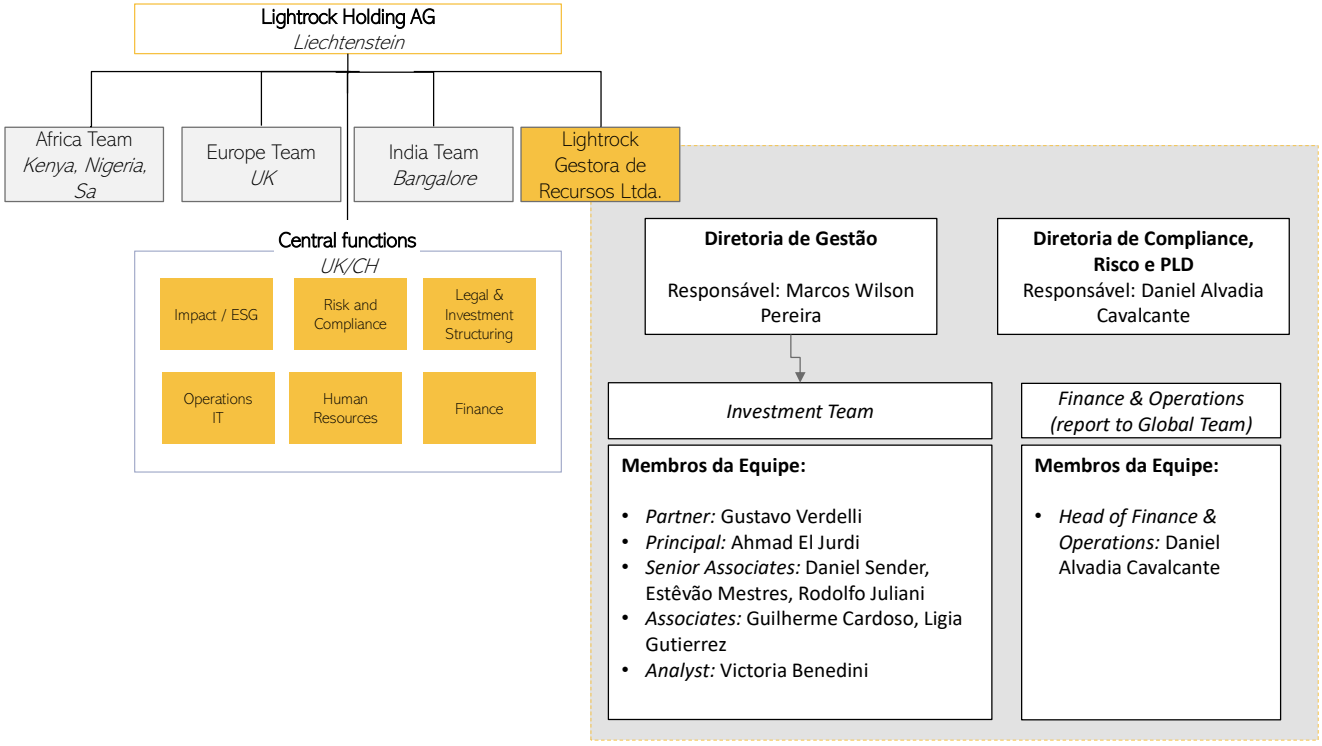
São descritas, abaixo, as principais funções de cada uma das diretorias:

- Diretoria de Gestão de Recursos: responsável pela gestão de carteiras administradas, a qual deverá ser realizada de acordo com estratégias, análises setoriais e de ativos financeiros e *private equity*. A diretoria é liderada pelo "Diretor de Gestão"; designado diretamente no contrato social da Gestora, nos termos do art. 4º, inciso III e parágrafo 7º, da ICVM 558/15;

- Diretoria de *Compliance*, Risco e PLDFT: responsável (i) pela gestão de riscos das carteiras administradas pela Gestora e monitoramento de risco dos ativos financeiros, conforme descrito na Política de Gestão de Riscos da Gestora, (ii) por desenvolver, aprovar, implementar e monitorar regras, políticas, rotinas e controles internos adequados aos padrões operacionais e de conduta legais e regulamentares, e (iii) pelo cumprimento das políticas, procedimentos e controles internos relativos à prevenção à lavagem de dinheiro e ao financiamento ao terrorismo. A diretoria é liderada pelo "Diretor de *Compliance*, Risco e PLDFT"; designado diretamente no contrato social da Gestora, nos termos do art. 4º, inciso IV e V e parágrafo 7º da ICVM 558/15, da ICVM 617/19 e da Lei 9.613.

Conforme aplicável, os especialistas locais e o time de suporte global oferecerão integral apoio e suporte às diretorias de forma autônoma, executando as tarefas e procedimentos operacionais, bem como desenvolvendo tarefas de *back office* essenciais ao desenvolvimento das atividades da Gestora.

O organograma da estrutura organizacional a ser adotada pela Gestora pode ser exposto da seguinte forma:



Sem prejuízo do disposto na presente Política, como entidade parte do Grupo Lightrock, a Gestora está sujeita ao disposto em políticas e códigos de conduta do Grupo Lightrock que estabelecem diretrizes e regras de Segurança da Informação aplicáveis a todos os colaboradores do Grupo Lightrock e suas afiliadas.

1.2. DISPOSIÇÕES GERAIS

1.2.1. DISPOSIÇÕES INICIAIS

Esta Política de Segurança da Informação destina-se aos Colaboradores da Gestora e deverá ser observado por todos.

Esta Política tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação, de acordo com a sensibilidade dos dados e das informações sob responsabilidade da Gestora. A segurança da informação ("Segurança da Informação") é aqui caracterizada pela preservação dos seguintes princípios:

a) **Confidencialidade:** é a garantia de que a informação é acessível somente por pessoas com acesso autorizado;

b) **Integridade:** é a garantia que a informação e os métodos de processamento deverão ser precisos, exatos, completos e atualizados; e

c) **Disponibilidade:** é a garantia de que os usuários autorizados obtenham acesso à informação armazenada e aos ativos correspondentes, sempre que necessário.

Para tornar a gestão da Segurança da Informação efetiva, a diretoria da Gestora coordena as ações necessárias para a implantação do modelo de gestão de Segurança da Informação e avalia periodicamente a Segurança da Informação, bem como recomenda ações corretivas e preventivas.

O Diretor de *Compliance*, Risco e PLDFT enquanto responsável pela presente Política de Segurança da Informação, ou outro Colaborador indicado por esse, com o auxílio do time de suporte Global, realizará as seguintes atividades:

a) Identificação das necessidades específicas de Segurança da Informação e proposta de implementações necessárias;

b) Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação;

c) Administrar e proteger as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Gestora;

d) Realização da gestão do plano de continuidade dos negócios;

e) Gerar as informações necessárias para auditoria com nível de detalhe suficiente para o rastreamento de possíveis falhas e fraudes;

f) Implantar controles de integridade para as informações armazenadas em meio eletrônico para que possam ser consideradas válidas como evidências;

g) Implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

h) Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Gestora; e

i) Análise dos incidentes de segurança da informação e recomendações de correções necessárias.

Compete ao Diretor de *Compliance*, Risco e PLDFT da Gestora a verificação do cumprimento da Política de Segurança da Informação e recomendação das ações corretivas necessárias. Assim, a Diretoria de *Compliance,* Risco e PLDFT contará com a solução de controle de navegação nas páginas da rede mundial de computadores, com política de perfis de acesso e governança, através de *firewall* configurável, será possível ter o controle de todos os acessos realizados pelos Colaboradores e Diretores da Gestora na *web*. Ou seja, será possível (i) a realização da análise do tráfego de informações pelos Diretores e Colaboradores e (ii) o veto de acesso a determinados canais de navegação (ex.: redes sociais e sites com conteúdo impróprio), de modo a auxiliar na constatação pela Diretoria de *Compliance,* Risco e PLDFT de eventuais acessos irregulares e em desacordo com a presente Política de Segurança da Informação.

Adicionalmente, as senhas de acessos dos Diretores e Colaboradores aos sistemas da Gestora irão expirar a cada 6 (seis) meses, sendo obrigatória a alteração

Esta Política de Segurança da Informação deve ser revisada na ocorrência de alterações materiais nas atividades, infraestrutura ou operações da Gestora. Entretanto, uma revisão mínima deve ocorrer a cada 3 (três) anos com o intuito de verificar a eventual necessidade de produzir uma versão atualizada, a ser aprovada pela Diretoria de *Compliance,* Risco e PLDFT da Gestora.

1.2.2. POLÍTICAS

Esta Política de Segurança da Informação será implementada na Gestora por meio de procedimentos específicos e obrigatórios para todos os Colaboradores, independentemente do nível hierárquico ou função instituição, bem como de vínculo empregatício ou prestação de serviços.

As seguintes diretrizes integram a Política de Segurança da Informação da Gestora:

a) **A informação pertence à organização:** Toda informação gerada, adquirida ou processada pela Gestora é de sua exclusiva propriedade. Deve-se haver uma comunicação prévia com a gerência imediata para a saída de documentos em meios físicos da instituição, que contenha informações críticas da Gestora;

b) **Segurança orientada ao negócio:** As ações de segurança serão planejadas e aplicadas de acordo com a avaliação dos riscos para o negócio da Gestora. A disponibilidade, uso, acesso e proteção das informações e seus recursos devem ocorrer sempre de forma a preservar a continuidade e a competitividade do negócio da Gestora;

c) **Propriedade da informação:** Toda informação armazenada nas dependências da Gestora é considerada patrimônio da Gestora, sendo usada exclusivamente em seu interesse e devendo estar adequadamente protegida, em qualquer que seja o meio de armazenamento, contra violação, alteração, destruição, acesso não autorizado e divulgação indevida. Os responsáveis por seu armazenamento, guarda e manuseio responderão por sua integridade, uso ou divulgação;

d) **Classificação da informação:** Cada Colaborador terá acesso às informações necessárias ao seu trabalho, respeitando os conceitos de Confidencialidade, Integridade e Disponibilidade;

e) **Responsabilidade:** Cada Colaborador é responsável pela segurança dos ativos e das informações que estejam sob sua custódia e por todos os atos executados com sua identificação de acesso. Qualquer que seja sua forma, a identificação será pessoal, intransferível e permitirá de maneira clara e indiscutível o seu reconhecimento;

f) **Menor privilégio:** O Colaborador terá acesso somente a ativos de informação que componham o imprescindível para o total desenvolvimento do seu trabalho;

g) **Cultura de segurança:** O conteúdo desta Política de Segurança da Informação e das demais normas será amplamente divulgado na Gestora;

h) **Recursos computacionais:** Os recursos computacionais disponibilizados pela Gestora devem ser utilizados apenas para o desenvolvimento de atividades relacionadas ao negócio da Gestora; e

i) **Treinamento em Segurança da Informação:** Os Colaboradores devem conhecer e respeitar a Política de Segurança da Informação da organização. Sempre que esta Política for revisada e atualizada, deverá ser realizado um programa de educação e treinamento, seja ele presencial ou remoto, para garantir a disseminação das informações atualizadas, bem como para assegurar o conhecimento e a compreensão das políticas e procedimentos de manutenção do sigilo e segregação de informações disponíveis em vigor, e da conscientização das consequências da não observância de referidas normas e procedimentos.

1.3. DISPOSIÇÕES FINAIS

1.3.1 CONSEQUÊNCIAS DO DESCUMPRIMENTO

A Gestora exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O descumprimento das políticas e procedimentos estabelecidos na presente Política de Segurança da Informação implicará nas seguintes medidas, segundo o entendimento do Diretor de *Compliance*, Risco e PLDFT (ou, caso o Diretor de *Compliance*, Risco e PLDFT esteja envolvido, de qualquer outro Diretor):

(i) demissão dos Colaboradores envolvidos no descumprimento em questão, incluindo aqueles que tinham conhecimento do descumprimento em questão e foram omissos em reportá-lo a seus superiores; e/ou

(ii) responsabilização dos Colaboradores envolvidos no descumprimento por eventuais danos que a Gestora venha a sofrer em razão de sua conduta.

A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e/ou criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos

resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos nesta Política de Segurança da Informação.