Nexus

Gestão de Ativos

Manual de *Compliance* e Segurança da Informação

Sumário

1. Objetivo

Este Manual tem por objetivo estabelecer as diretrizes e responsabilidades a serem observadas pela Nexus Tech Gestão de Ativos Ltda. (“Nexus Tech” ou “Gestora”) para o fortalecimento e aderência de seus negócios, de acordo com as regulamentações vigentes.

Estabelecer normas, princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança (“Colaboradores”) com a Gestora, tanto na sua atuação interna quanto na comunicação com os diversos públicos, visando ao atendimento de padrões éticos cada vez mais elevados.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Manual, informando qualquer irregularidade à Diretoria de Compliance e de Gestão de Risco, conforme definida no contrato social vigente da Nexus Tech (“Gestora).

2. Base Legal

- Item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014
- Resolução CVM nº 21, de 25 de fevereiro de 2021 com as alterações introduzidas pelas resoluções 162/22, 167/22 e 179/23
- Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“ANBIMA”) de Ética (“Código ANBIMA de Ética”)
- Código de Administração de Recursos de Terceiros (“Código de ART”)
- Código de Certificação (“Código ANBIMA de Certificação”)
- Lei nº 12.846/13 e Decreto nº 11.129/22 (“Normas de Anticorrupção”)
- Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Gestora
- Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (“LGPD”)

3. Diretrizes

São diretrizes básicas deste Manual:

- ✓ Monitorar diariamente o efetivo trancamento das estações de trabalho e backup de informações e, sempre que detectado algum desvio de conduta, voltar a instruir o colaborador a respeito das boas práticas de conduta;
- ✓ Verificar diariamente o eventual esquecimento de documentos em cima das mesas e/ou nas impressoras, instruindo os colaboradores sobre a necessidade de preservação das informações;

- ✓ Coordenar a promoção de testes periódicos de segurança para os sistemas de informações, em especial os mantidos em meio eletrônico e, inclusive, para os fins do Plano de Continuidade de Negócios adotada pela Sociedade.

3.1 Política de Segurança da Informação e Segurança Cibernética

As medidas de segurança da informação e segurança cibernética, têm por finalidade minimizar as ameaças aos negócios da Nexus Tech (gestora) e às disposições deste Manual, buscando, principal, a proteção de Informações Confidenciais.

As instalações da gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A Política de Segurança da Informação e Segurança Cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela gestora.

A coordenação direta das atividades relacionadas à Política de Segurança da Informação e Segurança Cibernética ficará a cargo da Diretoria de Compliance e de Gestão de Risco, que será a responsável, inclusive, por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

A quem se aplica?

A todos os Colaboradores, prestadores de serviços e clientes.

Responsabilidades

Os Colaboradores da Nexus Tech, devem atender às diretrizes e procedimentos estabelecidos nesta Política de Segurança da Informação e Segurança Cibernética, informando quaisquer irregularidades à Diretoria de Compliance e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de Compliance, Controles Internos, Ética e Risco, o qual decidirá sobre eventuais medidas cabíveis.

A Diretoria de Compliance e de Gestão de Risco deve garantir o atendimento a esta Política de Segurança da Informação e Segurança

Cibernética, sendo a responsável por temas de segurança da informação e segurança cibernética.

3.2 Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na Nexus Tech:

Confidencialidade: Acesso das informações apenas às pessoas autorizadas, ou seja, não disponibiliza esse acesso a indivíduos, entidades ou processos não autorizados.

Disponibilidade: As pessoas autorizadas devem ter acesso à informação sempre que necessário.

Integridade: A informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Do menor Privilégio: O acesso à informação deve ser obtido somente por pessoas autorizadas, e quando ele for de fato necessário;

As seguintes diretrizes devem ser seguidas por todos os Colaboradores:

- As Informações Confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;
- A concessão de acessos às Informações Confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Desta forma, há a segregação lógica das informações, de modo que e somente os Colaboradores autorizados têm acesso às pastas virtuais respectivas às suas atividades desenvolvidas na gestora;
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- Segregação de instalações, equipamentos e informações comuns, quando aplicável; e
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência, de falha na confidencialidade e na segurança da informação, devem ser reportados à Diretoria de Compliance e de Gestão de Risco, pelo responsável pelo Departamento de Procedimentos de Segurança Cibernética.

3.3 Identificação e Avaliação de Riscos (Risk Assesment)

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

- **Dados e Informações:** As Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- **Sistemas:** Informações sobre os sistemas utilizados pela gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- **Processos e Controles:** Processos e controles internos que sejam parte da rotina das áreas de negócio da gestora;
- **Governança da Gestão de Risco:** A eficácia da gestão de risco pela gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

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

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

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

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

3.4 Ações de Prevenção e Proteção

Uma importante regra de prevenção, consiste na segregação de acessos a sistemas e dados e de serviços que a gestora adota, sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamento relevantes. A gestora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do acesso.

A gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário. Ainda, a concessão de acesso pela gestora fora implementada de modo que pode ser revogada rapidamente, se necessário.

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

O acesso remoto a arquivos e sistemas internos ou na nuvem (*cloud*) é permitido, pois estes contam com controles adequados. O acesso ao acervo digital conta com dupla verificação. Quando o Colaborador acessa o *Office365* para acessar, é enviado um código de segurança no seu celular, garantindo a autenticidade.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A gestora ainda conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais. A gestora deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da gestora e circulem em ambientes externos à gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. qualquer exceção à presente regra deverá ser previamente autorizada por escrito pela Diretoria de Compliance e de Gestão de Risco.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da gestora.

Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar *pendrives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na gestora.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A gestora adota também backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de contingência e continuidade dos negócios da gestora, o backup de todos os dados e informações da gestora é realizado diariamente na nuvem.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo Informações Confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Art. 18 da Resolução CVM nº 21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são caras à prevenção e proteção dos ativos da gestora e devem ser observadas integralmente.

A gestora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade da gestora, mantendo inventários atualizados de hardware e software, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da gestora deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. Os logs e trilhas de auditoria criados devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

3.5 Monitoramento e Testes

A gestora adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual:

- Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos
- Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela gestora para a atividade profissional de cada colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da gestora;

- Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

A Área de Compliance e Risco poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

3.6 Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretoria de Compliance e Gestão de Risco prontamente.

A Diretoria de Compliance e Gestão de Risco levará tal questão ao Comitê de Compliance, Controles Internos, Ética e Risco, que determinará quais membros da administração da gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Comitê de Compliance, Controles Internos, Ética e Risco determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

3.7 Procedimentos de Resposta

A Diretoria de Compliance e Gestão de Risco responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da gestora de acordo com os critérios abaixo:

- Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
- Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
- Determinação dos papéis e responsabilidades do pessoal apropriado;
- Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
- Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, Autoridade Nacional de Proteção de Dados – ANPD, segurança pública), quando aplicável, especialmente em incidentes que envolvam dados pessoais;
- Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo informações confidenciais de fundo de investimento sob gestão da gestora, a fim de

garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

- Determinação do responsável (ou seja, a gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo da Diretoria de Compliance e Gestão de Risco, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.8 Processos e Controles de Segurança da Informação

Para assegurar que as informações sejam adequadamente protegidas, a gestora definiu os seguintes processos/controles:

Classificação da Informação

Algumas informações podem enquadrar-se como Informações Confidenciais. Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. Controles para Informações Classificadas como “Informações Confidenciais”

O acesso às Informações Confidenciais deve ser controlado. Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão da Diretoria de Compliance e de Gestão de Risco, e, se reputado necessário, da assessoria jurídica da gestora.

Salvaguarda da Informação

A informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento e descarte.

O Colaborador responsável pela informação gerada deve ter conhecimento do tempo regulatório de salvaguarda e gerenciar o seu armazenamento e descarte. Em caso de dúvida, o Colaborador deverá consultar a Diretor de Compliance e de Gestão de Risco.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na gestora são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia da Diretoria de Compliance e de Gestão de Risco. A gestora poderá, a qualquer momento e mediante prévia aprovação da Diretoria de Compliance e de Gestão de Risco:

- Inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;
- Disponibilizar esses recursos a terceiros, caso entenda necessário; e
- Solicitar aos usuários justificativas pelo uso efetuado.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

Boas Práticas de Utilização

A utilização da rede, internet, e-mail e dispositivos móveis na gestora e/ou pelos seus Colaboradores em comunicações de trabalho devem se guiar pelas seguintes regras:

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abri-la, para evitar vírus ou códigos maliciosos;
- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela gestora, nunca as repassar, alertando o responsável da sua área e a Diretoria de Compliance e de Gestão de Risco, se for o caso;
- Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho;
- Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail.

Vedações

É vedado ao usuário:

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais, sendo proibido, sobretudo, conteúdo pornográfico, racista, subversivo ou ofensivo à moral e aos princípios éticos;
- Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da gestora, ou qualquer outra informação

sobre a gestora, seus negócios, produtos, equipamentos ou Colaboradores, sem prévia aprovação para isso. Em caso de exigência de alguma autoridade ou entidade autorreguladora, solicitar orientação à Diretoria de Compliance e de Gestão de Risco;

- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados residentes na rede da gestora;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da gestora;
- Alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pela Diretoria de Compliance e de Gestão de Risco;
- Contratar provedores de acesso sem autorização prévia autorização da Diretoria de Compliance e de Gestão de Risco;
- Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na gestora e vice-versa.

3.9 Proteção de Dados Pessoais (LGPD)

A Nexus Tech, no exercício de suas atividades, coleta, armazena e realiza o tratamento de dados pessoais de clientes, investidores, Colaboradores, prestadores de serviços e demais partes relacionadas, em conformidade com a Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (“LGPD”) e com a regulamentação aplicável, incluindo, mas não se limitando, às normas da CVM sobre cadastro, identificação e qualificação de clientes e operações.

O tratamento de dados pessoais pela Gestora ocorre sempre dentro de finalidades legítimas, específicas e informadas, observando rigorosamente as bases legais previstas em lei e os princípios da LGPD.

Princípios e Finalidades do Tratamento

O tratamento de dados pessoais realizado pela Nexus Tech tem, entre outras, as seguintes finalidades:

- permitir a adequada prestação de serviços pela Gestora, inclusive a gestão de carteiras e de fundos de investimento sob sua responsabilidade;
- cumprir obrigações legais, regulatórias e autorregulatórias aplicáveis às atividades da Gestora;
- possibilitar a execução de contratos firmados com clientes, investidores, Colaboradores e prestadores de serviços;

- apoiar atividades de prevenção à lavagem de dinheiro, financiamento do terrorismo, combate à corrupção e demais controles de risco exigidos pela regulamentação vigente;
- proteger direitos da própria Gestora, de clientes, de investidores e de terceiros, inclusive em processos administrativos, arbitrais ou judiciais.

Os dados pessoais são coletados e utilizados apenas na extensão necessária para atender às finalidades acima, sendo vedado seu uso para propósitos incompatíveis ou não informados, bem como para benefício pessoal de Colaboradores ou terceiros.

Período de Tratamento e Armazenamento

Os dados pessoais tratados pela Nexus Tech serão mantidos:

- enquanto perdurar a relação contratual ou o vínculo que justificou sua coleta; e/ou
- pelo prazo exigido por leis, regulamentos ou normas autorregulatórias aplicáveis às atividades da Gestora; e/ou
- pelo período necessário para resguardar direitos da Gestora em processos administrativos, judiciais ou arbitrais.

Encerradas as finalidades ou decorrido o prazo legal ou regulatório aplicável, os dados pessoais serão eliminados, anonimizados ou tratados de acordo com as hipóteses previstas na LGPD e na regulamentação pertinente.

Direitos dos Titulares de Dados

Nos termos da LGPD, os titulares de dados pessoais tratados pela Nexus Tech podem exercer, dentre outros, os seguintes direitos:

- Confirmação e acesso: solicitar confirmação da existência de tratamento e acesso aos dados pessoais de sua titularidade;
- Correção: requerer a correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação: solicitar a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Portabilidade: requerer a portabilidade de seus dados pessoais a outro fornecedor de serviços ou produtos, observadas as normas da autoridade competente e os segredos comercial e industrial;
- Informação: obter informação sobre as entidades públicas e privadas com as quais a Gestora realizou uso compartilhado de dados;
- Eliminação de dados tratados com consentimento: solicitar a eliminação de dados pessoais tratados com base em consentimento, ressalvadas as hipóteses de guarda obrigatória ou de uso legítimo pela Gestora;

- Revogação do consentimento: revogar consentimento previamente concedido, nos termos da regulamentação aplicável.

Os pedidos relacionados ao exercício de direitos de titulares serão avaliados pela Diretoria de Compliance e de Gestão de Risco, ou por área por ela designada, observadas as hipóteses legais de manutenção e retenção de dados.

Compartilhamento de Dados Pessoais

A Nexus Tech poderá compartilhar dados pessoais com:

- administradores, custodiante, intermediários, prestadores de serviços e demais terceiros necessários à execução de seus serviços;
- autoridades regulatórias, autorregulatórias, fiscais e demais órgãos públicos, quando exigido por lei, regulamento ou decisão de autoridade competente;
- prestadores de serviço de tecnologia, armazenamento em nuvem, contabilidade, auditoria, consultoria e outros estritamente necessários às atividades da Gestora.

O compartilhamento será sempre realizado nos limites das finalidades indicadas e das bases legais aplicáveis, buscando assegurar a proteção e a confidencialidade dos dados pessoais compartilhados.

Segurança da Informação aplicada a Dados Pessoais

As medidas de segurança da informação e segurança cibernética previstas neste Manual aplicam-se também aos dados pessoais sob guarda da Nexus Tech, de forma a:

- proteger os dados contra acessos não autorizados, vazamentos, perdas, destruição ou qualquer forma de tratamento inadequado ou ilícito;
- restringir o acesso aos dados pessoais apenas a Colaboradores ou terceiros que deles necessitem para o desempenho de suas funções, observando o princípio do menor privilégio;
- manter registros e trilhas de auditoria adequados para possibilitar a verificação de acessos e incidentes de segurança.

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais, a Diretoria de Compliance e de Gestão de Risco avaliará a necessidade de adoção de medidas adicionais, incluindo a comunicação aos titulares afetados e à Autoridade Nacional de Proteção de Dados – ANPD, na forma da legislação aplicável.

Responsabilidade pela Proteção de Dados Pessoais

A Diretoria de Compliance e de Gestão de Risco é responsável, no âmbito da Nexus Tech, por supervisionar o cumprimento destas diretrizes relacionadas à proteção de dados pessoais, cabendo-lhe:

- orientar os Colaboradores quanto às obrigações decorrentes da LGPD;
- zelar pelo tratamento adequado, legítimo e seguro dos dados pessoais coletados e tratados pela Gestora;
- coordenar, quando necessário, a resposta a incidentes de segurança que envolvam dados pessoais.

4. Informação Privilegiada (*"Insider Information"*)

É terminantemente proibido o uso ou a divulgação de informação privilegiada por qualquer profissional vinculado a Nexus Tech, seja por atuação em benefício próprio ou de terceiros. As violações às exigências relacionadas ao uso de informações privilegiadas estarão sujeitas as penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria de *Compliance* da Nexus Tech.

Considera-se informação privilegiada qualquer informação relevante a respeito de qualquer sociedade ou negócio que envolva a Nexus Tech, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada, em decorrência da relação profissional ou pessoal mantida com um cliente, com colaboradores de empresas analisadas ou investidas ou com terceiros.

São exemplos de informações privilegiadas: informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários e, ainda, qualquer informação que seja objeto de um acordo de confidencialidade firmado pela Nexus Tech com terceiros.

As informações privilegiadas devem ser mantidas em absoluto sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

A pessoa que tiver acesso a uma informação privilegiada deverá divulgá-la, de forma imediata, à Diretoria de *Compliance* que é o responsável pela aplicação deste Manual, não devendo divulga-la a ninguém, nem mesmo a outros colaboradores da Nexus Tech, profissionais de mercado, amigos e parentes, e nem as utilizar em benefício próprio ou de terceiros.

A Diretoria de *Compliance* analisará a suposta informação privilegiada que foi divulgada pelo colaborador da Nexus Tech e, caso julgue que tal informação possa realmente ser classificada como tal, informará aos gestores de todos os produtos geridos pela Nexus Tech que tais produtos estão proibidos de

negociarem ações ou quaisquer outros títulos de companhias cujos valores possam ser afetados pela divulgação de tal informação privilegiada.

Quando a Diretoria de *Compliance*, responsável pela aplicação deste Manual, entender que tal informação privilegiada não poderá mais afetar os valores das ações e/ou títulos das companhias em questão, ele informará imediatamente a todos os gestores de produtos feridos pela Nexus Tech que tais ações e/ou títulos estão liberados para negociação por tais produtos.

Nos casos em que houver dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deverá, imediatamente, relatar tal fato à Diretoria de *Compliance* responsável pela aplicação deste Manual. Todo aquele que tiver acesso a uma informação privilegiada deverá limitar ao máximo a circulação de arquivos e/ou documentos que contenham tal informação.

Existem normas que proíbem a compra, venda, recomendação ou outros tipos de transferência de títulos e valores mobiliários em situações de conhecimento privilegiado de informações, ou seja, que não sejam de domínio público, sobre o emissor desses títulos.

Essas normas também vedam a revelação dessas informações a terceiros que possam comercializar tais títulos. As consequências da utilização de “informações privilegiadas” podem ser graves tanto para o colaborador quanto para a Nexus Tech.

Os colaboradores que tenham acesso às informações privilegiadas e/ou àquelas que ainda não tenham sido divulgadas ao público investidor, devem garantir o sigilo das mesmas, exceto quando necessária para a condução dos negócios da instituição e, ainda, somente caso não haja indícios para presumir que o receptor da informação a utilizará erroneamente.

As violações relacionadas às exigências quanto ao uso de informações privilegiadas estarão sujeitas as penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria de *Compliance* da Nexus Tech.

5. Confidencialidade e Sigilo das Informações

A Confidencialidade é um princípio essencial para a Nexus Tech. Deve ser aplicado a toda informação não pública que faça alusão a Nexus Tech, bem como às informações recebidas de clientes ou fornecedores para um objetivo comercial expresso.

A Nexus Tech, protege o sigilo e a privacidade das informações pessoais e financeiras de seus clientes, tratando todas as informações fornecidas como sigilosas, não sendo, portanto, permitida sua transmissão a terceiros, exceto mediante expressa e prévia anuência do cliente.

Os colaboradores da Nexus Tech, devem proteger o sigilo e a confidencialidade das informações referentes aos clientes, obtidas no desenvolvimento das atividades relacionadas à Nexus Tech.

O sigilo e a confidencialidade devem ser mantidos mesmo após o rompimento do vínculo, por qualquer motivo, com a Nexus Tech. A não observância da confidencialidade estará sujeita à apuração de responsabilidades na esfera cível e criminal.

Todas as informações, documentos, cópias e extratos originados nas atividades da Nexus Tech são de propriedade da Nexus Tech e deverão permanecer, única e exclusivamente, com a Nexus Tech. Os colaboradores, no término de sua relação com a Nexus Tech, devolverão a Nexus Tech todos os originais e todas as cópias de quaisquer documentos recebidos ou adquiridos durante o vínculo mantido com a Nexus Tech, bem como todos os arquivos, correspondências e/ou outras comunicações recebidas, mantidas e/ou elaboradas durante o respectivo vínculo com a Nexus Tech.

Qualquer divulgação de informações a autoridades governamentais em virtude de decisões judiciais, arbitrais ou administrativas que envolva, direta ou indiretamente, as atividades desenvolvidas pela Nexus Tech, deverá ser prévia e oportunamente relatada à Diretoria de *Compliance* responsável pela aplicação deste Manual, para que este decida sobre a forma mais adequada para tal divulgação.

Considerando a alta especialização da atividade desenvolvida pela Nexus Tech, bem como os princípios que regem o mercado de valores mobiliários, é definitivamente vedada a revelação de carteiras e estratégias de investimento de todo e qualquer produto analisado, administrado e/ou gerido pela Nexus Tech a qualquer não colaborador da Nexus Tech, seja da imprensa, seja do círculo pessoal de convívio, de ligação imediata de parentesco ou de estado civil. A não observância deste item estará sujeita à apuração de responsabilidades nas esferas civil e criminal.

As informações sobre a Nexus Tech devem ser transmitidas apenas nos casos que vierem a favorecer os fundos geridos pela Nexus Tech. A transmissão dessas informações deve ser realizada com o entendimento expresso de que as mesmas são confidenciais e devem ser utilizadas exclusivamente para o objeto restrito para o qual foram recebidas ou concedidas. Salvo instrução legal em contrário, informações de caráter confidencial somente poderão ser utilizadas para fins profissionais e sob nenhuma circunstância deverá ser utilizada para a obtenção de quaisquer vantagens pessoais.

Adicionalmente, é vedada a divulgação desse tipo de informação para terceiros ou profissionais não envolvidos e/ou autorizados a recebê-la.

Todos os colaboradores da Nexus Tech são responsáveis pela guarda de documentos relativos às suas atividades, devendo, portanto, garantir que informações confidenciais não sejam expostas a outros profissionais ou a

terceiros em trânsito na Nexus Tech em períodos de ausência de seu local físico de trabalho.

A Nexus Tech adota rigorosas normas para a proteção de informações confidenciais de clientes e tem como política o não fornecimento e a não divulgação de quaisquer informações a respeito de contas, investimentos, valores, volumes e dados cadastrais de seus clientes a terceiros, exceto se houver determinação do Poder Judiciário.

Todo o colaborar possui acesso controlado nos respectivos diretórios de acesso às informações, sendo identificados com login individual, podendo ser monitorado pelas áreas de TI e Compliance.

Portanto, o colaborador tem o compromisso de não divulgar a terceiros, direta ou indiretamente, mediante dolo ou culpa, durante o período em que estiver prestando serviços à Nexus Tech, e após o seu término, de qualquer informação confidencial ou documentos por ele elaborados no desempenho de suas funções, devendo mantê-las sob o mais absoluto sigilo.

O não cumprimento das exigências relacionadas à confidencialidade das informações estará sujeito a penalidades civis e criminais, multas e prisão, podendo ainda ser impostas sanções administrativas a critério da Diretoria de *Compliance* da Nexus Tech.

6. Sistema de Informação

São considerados Sistema de Informação todos os programas de Informática, incluindo, sem limitação, os e-mails, os sistemas instalados nos computadores de propriedade da Nexus Tech, bem como os bancos de dados que a Nexus Tech utiliza para o armazenamento de suas informações e das informações de seus clientes, e os sistemas que venham a ser desenvolvidos, direta ou indiretamente, pela equipe da Nexus Tech.

Todos os equipamentos e computadores de propriedade da Nexus Tech, assim como os bancos de dados utilizados pela Nexus Tech que forem disponibilizados aos colaboradores, deverão ser utilizados de forma a atender exclusivamente as finalidades da Nexus Tech.

A obtenção de cópias de arquivos de qualquer extensão, de forma gratuita ou remunerada, em computadores da Nexus Tech, originados em máquina remota (“*Download*”) dependerá de autorização expressa e previa da área responsável e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes.

Sob nenhuma circunstância será permitida a cópia de *softwares* piratas ou que não respeitem os direitos de propriedade intelectual, bem como aqueles que firam os bons costumes ou que promovam discriminação de qualquer tipo ou espécie.

A Nexus Tech disponibiliza endereço eletrônico a todos os colaboradores, sendo tal endereço eletrônico destinado para fins corporativos (“E-mail Corporativo”). A utilização do endereço eletrônico deverá ser feita para questões relacionadas às atividades profissionais e relacionadas à finalidade da Nexus Tech, sendo, no entanto, permitida a utilização pessoal, desde que de forma moderada.

Os E-mails Corporativos enviados ou recebidos, bem como seus respectivos anexos e os arquivos constantes nos computadores de propriedade da Nexus Tech poderão ser monitorados pela Nexus Tech.

Perante a possibilidade de acesso aos e-mails e arquivos, os colaboradores da Nexus Tech não devem manter nos computadores de propriedade da Nexus Tech qualquer dado ou informação particular que não pretendam que seja conhecida e/ou acessada pela Nexus Tech.

Todos os E-mails Corporativos recebidos pelos colaboradores da Nexus Tech, quando abertos, deverão ter sua adequação as regras deste Manual imediatamente verificada. Não será permitido, sob qualquer hipótese, a manutenção ou o arquivamento de mensagens cujo conteúdo seja ofensivo, discriminatório, pornográfico o vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

É permitida a utilização somente do programa de conversas eletrônicas (“*Chat*”) disponibilizado pela Nexus Tech, sendo permitido o seu uso para fins pessoais, desde que de forma moderada e dentro dos princípios e regras expostos no presente Manual. Toda a utilização do programa de conversas eletrônicas poderá ser monitorada pela Nexus Tech.

A navegação pela rede mundial de computadores (“*Internet*”) deverá ser feita observando os fins sociais da Nexus Tech, sendo permitido o seu uso para fins pessoais de forma moderada, como por exemplo, mas não se limitando, a compras de objetos de uso pessoal, passagens e reservas de hotéis.

A Nexus Tech reserva-se ao direito de bloquear sites da *Internet* que considere inapropriados ou que firam a moral e os bons costumes. Toda a navegação na *Internet* poderá ser monitorada pela Nexus Tech.

Os colaboradores deverão zelar pela conservação do computador utilizado, devendo, para tanto, realizar, periodicamente, a verificação da existência de vírus, bem como a manutenção do antivírus atualizado. Sendo constatada a presença de vírus ou qualquer anomalia, o colaborador deverá comunicar imediatamente o responsável da área.

As senhas de caráter sigiloso, pessoal e intransferível, serão fornecidas aos colaboradores da Nexus Tech para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo. É expressamente proibida a transmissão de senhas a terceiros, sendo os colaboradores da Nexus Tech responsáveis pela manutenção de cada senha com suas características.

A Nexus Tech entende ser imprescindível certas ligações telefônicas particulares, não significando que a ausência de bom senso por parte de seus colaboradores possa ser tolerada.

Ligações pessoais interurbanas e para celulares devem durar o tempo estritamente necessário e as ligações internacionais pessoais deverão ser prontamente reembolsadas a Nexus Tech.

Em caso de visitas particulares, os colaboradores da Nexus Tech deverão recebê-las apenas nas salas de reuniões, a fim de assegurar o sigilo total das informações referentes às operações e clientes envolvidos.

6.1 Sites de Armazenamentos de Arquivos

O acesso a sites de armazenamento de arquivos em “nuvem” é permitido. Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à gestora.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da gestora, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas à Diretoria de Compliance e de Gestão de Risco, que poderá ou não conceder a exceção.

6.2 Rastreamento

É permitido o uso pessoal dos equipamentos de informática e de comunicação de propriedade da gestora utilizados pelos colaboradores para a realização das atividades profissionais, lembrando que, como tais recursos (e-mails, sistemas, computadores, telefones etc.) pertencem à gestora, estes são rastreáveis e sujeitos a monitoramento, nos termos já dispostos neste Manual, bem como podem se tornar públicos em caso de auditoria, exigência judicial e/ou regulatória.

6.3 Treinamento

A Diretoria de Compliance e de Gestão de Risco organizará treinamento anual dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de compliance (conforme descrito abaixo).

6.4 Revisão e Atualização

Esta Política de Segurança da Informação e Segurança Cibernética deverá ser revisada e atualizada, caso necessário, anualmente, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatórias e/ou complementações.

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

7. Segurança da Informação

Compete ao *Compliance,* adotar todos os controles necessários para assegurar o sigilo das informações de acordo com os princípios estabelecidos nesse manual. Segue abaixo as rotinas da área no que se diz respeito à segurança das informações:

- Monitorar diariamente o efetivo trancamento das estações de trabalho e backup de informações e, sempre que detectado algum desvio de conduta, voltar a instruir o colaborador a respeito das boas práticas de conduta;
- Verificar diariamente o eventual esquecimento de documentos em cima das mesas e/ou nas impressoras, instruindo os colaboradores sobre a necessidade de preservação das informações;
- Coordenar a promoção de testes periódicos de segurança para os sistemas de informações, em especial os mantidos em meio eletrônico e, inclusive, para os fins do Plano de Continuidade de Negócios adotada pela Sociedade.

8. Segregação das Atividades

As áreas de administração de carteiras da Nexus Tech estão localizadas em uma área distinta das demais áreas da empresa.

Os arquivos digitais da Nexus Tech são restritos a cada área, de forma que quando um colaborador é admitido ou transferido para uma área na qual não possui acesso aos arquivos, o gestor responsável pela área e o Diretor de Compliance precisam validar a liberação para o colaborador.

Todos os arquivos digitais que possuem algum tipo de cunho confidencial possuem acesso restrito, de forma que o colaborador permitido ao acesso precisa de um login e senha para visualizar o arquivo. Além disso, os arquivos físicos das áreas de administração de carteiras ficam em local distinto dos outros arquivos e é necessária autorização da área para ter acesso ao arquivo.

9. Comunicação com a Imprensa – Divulgações Públicas

Somente estão autorizadas a fazer declarações ou conceder entrevistas a jornalistas, repórteres entrevistadores, agentes da imprensa falada ou escrita, em nome da Nexus Tech, os Diretores, o responsável pela área de marketing e os colaboradores indicados expressamente por estes à jornalistas, repórteres, entrevistadores ou agentes da imprensa falada ou escrita.

Os colaboradores da Nexus Tech autorizados a fazer declarações ou conceder entrevistas devem limitar-se a tecer comentários estritamente técnicos, de forma cautelosa, evitando-se o uso de juízos de valor desnecessário.

É proibido, sob qualquer circunstância, fazer declarações que possam aparentar ou ter conteúdo discriminatório no que diz respeito à raça, religião, cor, origem, idade, sexo, deficiência ou de qualquer outra forma não autorizada expressamente em Lei, assim como as que indiquem, direta ou indiretamente, posição político-partidária.

10. Divulgação de Informações Financeiras

Toda e qualquer informação financeira que diz respeito à Nexus Tech é confidencial, a não ser que tenha sido objeto de divulgação através de relatórios publicados em jornais ou outros veículos de comunicação.

Excetua-se ao caso acima quando este tipo de informação é requisitado por órgão regulador ou com prévia aprovação da Diretoria de *Compliance*.

11. Propriedade Intelectual

A Nexus Tech é detentora dos direitos de propriedade de quaisquer materiais, produtos ou serviços que sejam criados durante a jornada regular de trabalho e/ou que tenham sido produzidos fazendo-se o uso de ativos ou recursos da instituição.

Qualquer pessoa que, intencionalmente malversar, furtar ou se apropriar de maneira fraudulenta de qualquer quantia, recurso financeiro ou ativo de valor pertencente à Nexus Tech, ficará sujeita, além das sanções disciplinares, aos rigores da legislação aplicável.

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à gestora, tais como minutas de contrato, memorandos, cartas, *facsímiles,* apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da gestora, razão pela qual o colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na gestora, devendo todos os documentos permanecer em poder e sob a custódia da gestora, sendo vedado ao colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da gestora, salvo se autorizado expressamente pela gestora e ressalvado o disposto abaixo.

Caso um colaborador, ao ser admitido, disponibilize à gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou

ferramentas similares para fins de desempenho de sua atividade profissional junto à gestora, o colaborador deverá comunicar a diretoria de Risco e Compliance, declarando que:

- A utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;
- Quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da gestora, sendo que o colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da gestora, exceto se aprovado expressamente pela gestora.

12. Legislação, Normas e Outras Diretrizes

Existem diversas leis federais, estaduais, municipais e normas regulamentares aplicáveis ao campo de atividades da Nexus Tech. Todas têm ampla divulgação tanto no mercado financeiro, quanto internamente, sendo responsabilidade de todos os colaboradores estarem atualizados e conduzirem seus negócios em conformidade com às mesmas.

Em caso de dúvidas quanto ao cumprimento destas normas, essas devem ser esclarecidas junto à Diretoria de *Compliance*, pelos Departamentos Jurídico e de Recursos Humanos da Nexus Tech.

No âmbito da Nexus Tech existem também alguns regulamentos internos e manuais corporativos aprovados pela e que devem ser respeitados, de valor e grau de igualdade.

13. Proteção e Uso dos Ativos da Instituição

A Nexus Tech fornece diversas ferramentas de trabalho aos seus colaboradores de modo a auxiliá-los no desempenho de suas tarefas, sendo a propriedade da Nexus Tech deve ser adequadamente utilizada e protegida.

Entende-se por propriedade todos os tipos de bens, incluindo equipamentos, materiais e bens imobiliários, bem com as informações e outras propriedades intelectuais.

É dever dos colaboradores envidar esforços para proteger os ativos da instituição e garantir seu bom uso.

Qualquer suspeita de fraude ou furto deve ser comunicada imediatamente à Diretoria de *Compliance*.

Os materiais e equipamentos não devem ser utilizados para negócios não relacionados às atividades da Nexus Tech, salvo para uso particular do

colaborador, que poderá ser objeto de autorização expressa da Diretoria de *Compliance*.

Por motivos de segurança, o uso dos computadores, principalmente a utilização de serviços de correio eletrônico e *internet*, assim como o uso de telefones, estarão sujeitos ao monitoramento e supervisão por parte da Nexus Tech, independentemente de aviso prévio.

A *internet* deve ser usada para fins profissionais.

Está permanentemente proibido aos colaboradores a utilização dos equipamentos da Nexus Tech para:

- Acessar sites que contenham materiais obscenos, lascivos, pornográficos, preconceituosos, difamatórios ou qualquer outro conteúdo que afronte os princípios éticos e morais;
- Receber e enviar mensagens eletrônicas com conteúdo obsceno, pornográfico, preconceituoso e difamatório;
- Fins ilícitos;
- Dar opiniões pessoais ou fazer declarações em nome da Nexus Tech; e
- Copiar e/ou utilizar materiais, documentos e sistemas (*softwares*) com direitos autorais pertencentes a terceiros.

Os *e-mails* do domínio “nexustech.ia.br” pertencem a Instituição, sendo que, conforme determinação da Diretoria de *Compliance*, o colaborador poderá ou não receber uma caixa postal neste domínio. Esta caixa postal se submeterá as regras deste Manual.

Lembramos que, os serviços e recursos disponibilizados pela Nexus Tech, são para uso estritamente profissional, podendo a Instituição restringir, aumentar, fiscalizar, monitorar ou impedir a utilização dos mesmos a qualquer tempo.

14. Relacionamento com Fornecedores, Clientes, Concorrentes, Parceiros e Órgãos Fiscalizadores

É proibido solicitar ou aceitar para si próprio ou terceiros quaisquer itens de valor em troca de negócios com a Nexus Tech, favorecimento pessoal ou fornecimento de informação confidencial.

Consideram-se como itens de valor os abaixo citados:

- Dinheiro ou outras formas de remuneração, tais como gratificações, gorjetas, etc.;
- Títulos;
- Oportunidades de negócios;
- Mercadorias e serviços;
- Entretenimento;
- Alimentos;

- Bebidas.

Os colaboradores, obrigam-se a reportar aos Diretores da Gestora, caso recebam qualquer presente ou brinde em razão da posição ocupada por este na mesma, inclusive de clientes, fornecedores ou prestadores de serviços.

15. Disposições Gerais

Este documento foi elaborado pelos departamentos de *Compliance* encontra-se disponível para consulta pública, em sua versão integral e atualizada, no website da Gestora: https://nexustech.capital/.

ANEXO I

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, doravante denominado Colaborador, e Nexus Tech Gestão de Patrimônio Ltda., inscrita no CNPJ 17.055.372/0001-18, Administradora de Carteira autorizada pela Comissão de Valores Mobiliários (CVM) através do Ato Declaratório nº 16555 de 2018, sediada na Avenida Fausto Pietrobom, n° 414, Jardim Planalto, cidade de Paulínia, SP, ora denominada “Nexus Tech”.

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da GESTORA, incluindo dados pessoais tratados nos termos da Lei nº 13.709/18 (“LGPD”) e da Política de Proteção de Dados Pessoais da Nexus Tech celebrar o presente termo de confidencialidade (“Termo”), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas (“Informações Confidenciais”), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da GESTORA, incluindo:

a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora;

c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora;

d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;

e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;

f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

g) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador, compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, *fac-símiles*, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, em especial do Manual de Compliance e Segurança da Informação da Nexus Tech, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[local], [data].

_____

[COLABORADOR]