



BlueOak Investments Asset Ltda.

Política de Segurança da Informação e Cibernética

Este documento foi desenvolvido e é atualizado pela BlueOak Investments Asset Ltda. (“BlueOak”). Este documento está sujeito a alterações sem aviso prévio. É vedada a reprodução, alteração e transmissão por qualquer forma ou meio deste documento, em parte ou em sua totalidade, sem a autorização expressa da BlueOak.

Avenida Cidade Jardim, nº 400, 12º andar
Jardim Paulistano – São Paulo SP
01454-901 - Brasil

Telefone: +55 11 3031-5252

www.BlueOak.com.br

1. Introdução

A presente Política de Segurança da Informação e Cibernética (“Política”) foi elaborada pela BlueOak Investments Asset Ltda. (“BlueOak”) em conformidade com a legislação e regulamentação aplicáveis, considerando a natureza de suas atividades e os riscos inerentes ao tratamento de informações e ao uso de recursos tecnológicos. A presente Política estabelece princípios, diretrizes e responsabilidades relacionados à proteção das informações, ao uso adequado de sistemas, equipamentos e ferramentas tecnológicas disponibilizadas pela BlueOak, bem como às práticas de segurança da informação e cibernética adotadas pela instituição.

As diretrizes previstas nesta Política foram definidas a partir da avaliação dos riscos associados às atividades da BlueOak, tendo por objetivo prevenir, identificar e mitigar riscos relacionados à segurança da informação e à proteção de dados.

O descumprimento das disposições desta Política poderá ensejar o Colaborador às medidas disciplinares previstas no Código de Ética e Conduta da BlueOak, sem prejuízo da eventual responsabilização civil, administrativa ou criminal, nos termos da legislação e regulamentação aplicáveis.

Esta Política deverá ser interpretada em conjunto com o Código de Ética e Conduta da BlueOak e com as demais políticas, regras, procedimentos e controles internos da instituição.

2. Histórico de Versões

Versão	Data de Aprovação	Área Responsável	Justificativa
1.0	17 de fevereiro de 2023	Departamento de Tecnologia de Informação e Departamento de Risco e Compliance	Versão inicial
2.0	23 de abril de 2023	Departamento de Tecnologia de Informação e Departamento de Risco e Compliance	Alteração decorrente do ofício de exigência ANBIMA nº 01/044482/2023, expedido em 3 de abril de 2023, no âmbito do pedido de credenciamento para o exercício profissional da atividade de administração de carteira de valores mobiliários.
3.0	17 de agosto de 2026	Departamento de Tecnologia de Informação e Departamento de Risco e Compliance	Atualização e Revisão

3. Revisão e Aprovação

Esta Política será revisada pelo Departamento de Tecnologia da Informação (“DTI”) em conjunto com o departamento jurídico da BlueOak periodicamente sempre que se faça necessário, inclusive em decorrência de alteração da regulamentação em vigor aplicável ou, ainda, de aspectos relativos às atividades desempenhadas pela BlueOak e seus Colaboradores e/ou à infraestrutura tecnológica de segurança da informação ou cibernética, não sendo obrigatória a revisão em periodicidade mínima fixa.

O DTI informará ao Departamento de Risco e Compliance da BlueOak (“DRC”) a conclusão da revisão desta Política, ainda que não tenham sido identificadas alterações relevantes.

4. Abrangência

Esta Política se aplica a todos os sócios, administradores, empregados, estagiários, diretores e demais colaboradores da BlueOak (“Colaboradores”). Todos os Colaboradores devem se assegurar do pleno conhecimento e atendimento da legislação e regulamentação aplicáveis às suas funções, bem como do conteúdo integral desta Política.

5. Definições

Para fins desta Política, os termos abaixo terão as seguintes definições:

- Backup: atividade que consiste na realização de cópias de segurança de dados digitais com o objetivo de possibilitar sua recuperação em caso de perdas acidentais, falhas de sistema ou outros incidentes;
- Mídias Removíveis: dispositivos que permitem a leitura e gravação de dados, tais como HD externo, CD, DVD, pendrive, cartão de memória, entre outros;
- USB: modalidade de conexão de periféricos sem a necessidade de desligar o computador;
- Ferramentas de Inteligência Artificial: plataformas, aplicações, modelos generativos, assistentes virtuais ou quaisquer outras soluções tecnológicas capazes de produzir textos, imagens, códigos, análises, apresentações ou qualquer outro conteúdo mediante processamento automatizado de informações.
- Firewall: sistema de segurança de rede utilizado para controlar e restringir o tráfego de dados entre redes internas e externas, com o objetivo de proteger os sistemas e informações da BlueOak;
- IA Corporativa: ferramenta de Inteligência Artificial disponibilizada, contratada ou expressamente autorizada pela BlueOak para utilização pelos Colaboradores no exercício de suas funções.
- Ferramentas de Comunicação e Videoconferência: aplicações utilizadas para realização de reuniões virtuais, comunicação online e compartilhamento de informações, disponibilizadas ou autorizadas pela BlueOak;
- Informação Confidencial e Privilegiada: toda e qualquer informação produzida, recebida ou utilizada

pela BlueOak e pelos Colaboradores no exercício de suas respectivas funções na BlueOak, bem como toda e qualquer informação relevante e não pública cujo acesso seja restrito, assim consideradas informações que possam afetar decisões de investimentos ou negociação de valores mobiliários antes de sua divulgação ao mercado.

6. Princípios

A BlueOak compreende o dinamismo inerente ao mundo virtual e a facilidade envolvendo o acesso e a troca de informações.

Nesse contexto, o acesso e o compartilhamento de informações pelos Colaboradores no exercício de suas funções na BlueOak deverão ocorrer com estrita observância aos princípios, regras, políticas, procedimentos e controles internos adotados pela BlueOak, bem como com a legislação e regulamentação aplicáveis às suas atividades.

Neste sentido, a segurança da informação e cibernética da BlueOak é pautada nos seguintes princípios, os quais devem ser observados por todos os Colaboradores:

- (i) Confidencialidade: os Colaboradores devem garantir que Informações Confidenciais e Privilegiadas sejam acessadas apenas e somente por Colabores e/ou pessoas autorizadas e que delas necessitem para o exercício de suas funções;
- (ii) Integridade: os Colaboradores devem garantir que Informações Confidenciais e Privilegiadas não sejam alteradas, destruídas ou manipuladas de forma indevida ou não autorizada; e
- (iii) Disponibilidade: os Colaboradores devem garantir que Informações Confidenciais e Privilegiadas estejam disponíveis para acesso por Colaboradore e/ou pessoas autorizadas, quando necessário para o desempenho das atividades da BlueOak.

Para assegurar a observância de tais princípios, os Colaboradores deverão manusear, armazenar e proteger adequadamente as Informações Confidenciais e Privilegiadas contra acessos indevidos, perdas, vazamentos, fraudes ou outras ameaças. A utilização de Ferramentas de Inteligência Artificial deverá observar esta Política, o Código de Ética e Conduta, a legislação aplicável e as diretrizes estabelecidas pela BlueOak, preservando a confidencialidade, integridade, disponibilidade e proteção das informações.

7. Regras Gerais de Uso de Equipamentos, Ferramentas e Serviços

Os equipamentos de propriedade da BlueOak, assim como os serviços e ferramentas por ela contratados para o desempenho de suas atividades (incluindo, mas não se limitando, a softwares, serviços de correio eletrônico, internet e telefonia móvel), são de exclusiva propriedade da BlueOak e devem ser utilizados pelos Colaboradores (i) com diligência e zelo, de forma a preservá-los adequadamente conservandoos como se seus fossem; e (ii) única e exclusivamente, para fins de exercício de suas respectivas funções e no melhor interesse da BlueOak.

Os Colaboradores deverão observar, inclusive, mas não se limitando, as seguintes regras de uso dos equipamentos, ferramentas e serviços a eles disponibilizados pela BlueOak:

- (i) o acesso aos sistemas deverá ser realizado, quando aplicável, mediante login e senha

pessoais e intransferíveis;

- (ii) os equipamentos, ferramentas e serviços deverão ser utilizados em conformidade com as políticas, procedimentos e controles internos da BlueOak, incluindo o Código de Ética e Conduta, para fins de exercício de suas respectivas funções e visando tão somente o melhor interesse da BlueOak;
- (iii) somente poderão ser baixados (download) ferramentas, programas e softwares necessários ao exercício das respectivas funções desempenhadas pelos Colaboradores;
- (iv) os correios eletrônicos corporativos deverão ser utilizados de forma diligente, não sendo admitida a manutenção ou circulação de mensagens com conteúdo ofensivo, discriminatório, pornográfico, vexatório ou que possam representar risco à segurança da informação;
- (v) a instalação ou utilização de ferramentas, programas e softwares deverá observar as orientações e os padrões de segurança definidos pelo DTI;
- (vi) os Colaboradores deverão adotar práticas adequadas de segurança da informação no uso de equipamentos e sistemas, incluindo a proteção de acessos e o armazenamento seguro das informações e sempre que disponibilizadas pelo DTI, as atualizações de ferramentas, programas e softwares deverão ser realizadas conforme as orientações internas;
- (vii) os computadores (desktops e notebooks) deverão ser bloqueados e/ou desligados pelos Colaboradores mediante o encerramento de suas respectivas atividades, inclusive, mas não se limitando, na hipótese de pausas para cafés, lanches, almoços e reuniões internas e externas;
- (viii) os Colaboradores somente poderão utilizar ferramentas de Inteligência Artificial previamente disponibilizadas ou expressamente autorizadas pela BlueOak para fins profissionais;
- (ix) é vedado inserir, copiar, transcrever, carregar ("upload"), compartilhar ou de qualquer forma disponibilizar Informações Confidenciais, Privilegiadas, documentos internos, informações de clientes, investidores, fundos, operações ou quaisquer dados da BlueOak em ferramentas de Inteligência Artificial não autorizadas pela BlueOak;
- (x) é vedada a utilização de contas pessoais de ferramentas de Inteligência Artificial para atividades profissionais relacionadas à BlueOak; e
- (xi) conteúdos produzidos com auxílio de Inteligência Artificial deverão ser revisados criticamente pelo Colaborador responsável antes de sua utilização ou divulgação.

A BlueOak se reserva o direito de, a qualquer momento, monitorar o uso adequado de seus equipamentos, ferramentas corporativas e ferramentas de Inteligência Artificial pelos Colaboradores, disponibilizadas pela instituição, para fins de segurança da informação, gestão de riscos, observada a legislação aplicável, o Código de Ética e Conduta e a verificação do cumprimento desta Política.

O DRC disponibilizará aos Colaboradores, até a data de seu ingresso na BlueOak, uma cópia física ou digital desta Política. Os Colaboradores deverão, por ocasião de seu ingresso, assinar o “Termo de Adesão e Responsabilidade por Guarda e Uso de Equipamentos da BlueOak Investments Asset Ltda.”, conforme modelo constante do Anexo I desta Política (“Termo de Adesão e Responsabilidade”), o qual será arquivado pelo DRC em formato físico ou digital na sede da BlueOak.

8. Informações Confidenciais

Nos termos do Código de Ética e Conduta, todos os Colaboradores estão cientes da natureza confidencial das informações por eles produzidas, recebidas e/ou manipuladas no exercício de suas funções na BlueOak (“Informações”).

É vedada a utilização de ferramentas de Inteligência Artificial não autorizadas pela BlueOak para processamento, armazenamento, interpretação, resumo, tradução ou qualquer outro tratamento envolvendo Informações Confidenciais ou Privilegiadas. Ainda, sempre que utilizada ferramenta de Inteligência Artificial corporativa, o Colaborador deverá observar as limitações técnicas da ferramenta e realizar validação independente do conteúdo produzido.

Os Colaboradores deverão utilizar as Informações única e exclusivamente para o exercício de suas funções, abstendo-se de utilizá-las em benefício próprio ou de dar conhecimento das Informações a qualquer (i) pessoa que não seja um Colaborador, ressalvada a hipótese de disponibilização de Informações a prestadores de serviço da BlueOak que necessitem ter acesso a Informações para fins de cumprimento de seus serviços em benefício da BlueOak, desde que estejam sujeitos à obrigação de manter o sigilo das Informações, bem como nas hipóteses em que tal compartilhamento seja exigido por lei, regulamentação aplicável ou por autoridades competentes; e (ii) Colaborador que não necessite ter acesso às Informações para o exercício de suas funções. Nesse sentido, os Colaboradores estão terminantemente proibidos, ainda, de realizar cópias, backup e/ou gravação, por qualquer meio ou forma, de Informações para benefício próprio e/ou de terceiros, ressalvados os registros, cópias ou backups realizados em sistemas corporativos ou em conformidade com as políticas e procedimentos internos da BlueOak.

9. Utilização de Ferramentas de Inteligência Artificial

A BlueOak poderá disponibilizar ou autorizar a utilização de Ferramentas de Inteligência Artificial (“IA”) para apoio às atividades desempenhadas por seus Colaboradores, observado o disposto nesta Política, no Código de Ética e Conduta e na legislação aplicável.

Os Colaboradores somente poderão utilizar ferramentas de Inteligência Artificial disponibilizadas, contratadas ou expressamente autorizadas pela BlueOak para fins relacionados ao exercício de suas atividades profissionais.

É vedada a utilização de contas pessoais ou de ferramentas de Inteligência Artificial não autorizadas pela BlueOak para tratamento, armazenamento, análise, tradução, resumo, processamento, compartilhamento ou qualquer outra forma de utilização envolvendo Informações Confidenciais, Informações Privilegiadas, dados pessoais, documentos internos, operações, clientes, investidores, Fundos BlueOak ou quaisquer outras informações relacionadas às atividades da BlueOak.

Os Colaboradores permanecem integralmente responsáveis pela exatidão, qualidade, completude, legalidade e adequação de quaisquer documentos, análises, pareceres, comunicações ou demais materiais

produzidos com auxílio de ferramentas de Inteligência Artificial, devendo revisar criticamente todo conteúdo antes de sua utilização ou divulgação.

A utilização de ferramentas de Inteligência Artificial não afasta os deveres de confidencialidade, sigilo profissional, proteção de dados, prevenção de conflitos de interesses e observância das políticas internas da BlueOak.

O DRC poderá estabelecer requisitos técnicos, restrições de uso, controles de acesso, registros de utilização e procedimentos de monitoramento relativos às ferramentas de Inteligência Artificial disponibilizadas pela BlueOak, observada a legislação aplicável.

Qualquer utilização indevida de ferramentas de Inteligência Artificial, especialmente envolvendo informações confidenciais ou ferramentas não autorizadas, será considerada incidente de segurança da informação e deverá ser imediatamente comunicada ao DTI e ao DRC, sujeitando o Colaborador às medidas disciplinares cabíveis.

10. Acesso e Login/Senha

Os Colaboradores, quando do seu ingresso na BlueOak, receberão login e senha para acesso aos equipamentos, ferramentas e serviços corporativos da BlueOak, observado que, para fins de realização do primeiro acesso e início de suas atividades, os Colaboradores deverão alterar a senha por eles recebida por uma nova senha de sua livre escolha ou criada de acordo com os procedimentos e sistemas corporativos de autenticação adotados pela BlueOak, e de acordo com os parâmetros de eficácia e segurança informados abaixo.

O login e a senha são secretos, pessoais e intransferíveis, de forma que não poderão ser compartilhados pelos Colaboradores, sob qualquer hipótese, com qualquer outro Colaborador (inclusive, mas não se limitando, um Colaborador que seja sócio, administrador e/ou membro integrante do DRC ou do DTI), ressalvadas as hipóteses de acesso administrativo ou suporte técnico realizado pelo DTI, quando necessário para fins operacionais ou de segurança da informação.

A criação de nova senha pessoal pelos Colaboradores deve seguir os seguintes parâmetros para garantia de eficácia e de segurança:

- mínimo 8 (oito) caracteres;
- mínimo 1 (um) caractere especial (por exemplo, @, #, \$, %, !, &, etc.); e
- mínimo 1 (uma) letra maiúscula.

Ainda, na criação da nova senha pessoal, a BlueOak sugere sejam observadas as seguintes diretrizes pelos Colaboradores:

- utilização de uma senha diferente de outras senhas utilizadas pelos Colaboradores para acesso a outros ambientes protegidos;
- uso de números aleatórios;
- uso de grande quantidade de caracteres;

- uso de diferentes tipos de caracteres embaralhados;
- evitar uso de dados pessoais, tais como nomes, sobrenomes, datas de celebração, números de documentos, números de telefones e placas de carros;
- evitar senhas associadas à proximidade entre os caracteres no teclado, como por exemplo “qwertyuiop” ou “1qaz2wsx”; e
- evitar palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol e personagens de filmes.

A senha deverá ser alterada regularmente ou sempre que houver suspeita de comprometimento das credenciais, em periodicidade estabelecida pelo DTI.

11. Hábitos Recomendados

Com o objetivo de gerenciar e proteger adequadamente as Informações, é de suma importância que os Colaboradores adotem hábitos básicos de segurança no âmbito do exercício de suas funções, inclusive os seguintes, sem prejuízo da adoção de outros hábitos que visem a segurança das Informações:

- (i) manter a mesa de trabalho livre de documentos que possam conter Informação, especialmente quando não estiverem sendo utilizados ou quando houver ausência do Colaborador da estação de trabalho;
- (ii) utilizar tela com proteção de senha, sempre que se ausentar da estação de trabalho;
- (iii) configurar o computador (desktop ou notebook) para que realize bloqueio automático após 5 (cinco) minutos de inatividade;
- (iv) armazenar todos e quaisquer arquivos eletrônicos somente em locais autorizados e apropriados dentro da rede corporativa da BlueOak (não realizar o armazenamento de dados profissionais e Informações em equipamentos de uso pessoal);
- (v) não realizar o armazenamento de dados pessoais nos sistemas da BlueOak;
- (vi) descartar adequadamente arquivos físicos e eletrônicos que contenham Informações, de forma a impedir o conhecimento e leitura por terceiros. No caso de arquivos físicos, a BlueOak disponibilizará trituradores de documentos, os quais deverão ser devidamente utilizados pelos Colaboradores;
- (vii) não realizar conferências telefônicas ou videoconferências em locais públicos;
- (viii) adotar a máxima diligência, zelo e precauções ao falar em público sobre assuntos relacionados à BlueOak e suas atividades; e
- (ix) não utilizar ferramentas de Inteligência Artificial pessoais para armazenar, resumir, traduzir ou processar documentos corporativos.

Os hábitos descritos acima deverão ser observados pelos Colaboradores nas dependências da BlueOak, bem como na hipótese de exercício de suas funções na modalidade home office, conforme seja autorizado pela BlueOak. Caso a BlueOak autorize o trabalho na modalidade home office, os Colaboradores estão obrigados a tomarem os cuidados extras que a ocasião exige, sem prejuízo do disposto nesta Política.

12. Monitoramento, Inspeção e Testes

Nos termos do Código de Ética e Conduta, a BlueOak poderá (i) acessar as ferramentas de trabalho disponibilizadas aos Colaboradores para o exercício de suas funções, tais como celulares, desktops, notebooks e e-mails corporativos; e (ii) monitorar e rastrear a navegação virtual e as trocas de informações realizadas por meio de tais ferramentas de trabalho, observada a legislação aplicável e as políticas internas da BlueOak.

Ademais, a BlueOak poderá realizar periodicamente, a seu único e exclusivo critério, com o auxílio do DTI, (i) inspeções nas ferramentas de trabalho dos Colaboradores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos, bem como para a verificação da observância do disposto nesta Política. Poderão ser realizados, ainda, testes com o objetivo de detectar, em tempo hábil, anomalias no sistema tecnológico da BlueOak, como a presença de usuários, componentes ou dispositivos não autorizados, bem como outras vulnerabilidades ou riscos à segurança da informação.

O monitoramento poderá abranger, quando aplicável, a utilização das ferramentas de Inteligência Artificial corporativas disponibilizadas pela BlueOak, exclusivamente para fins de segurança da informação, compliance, auditoria e gestão de riscos.

13. Devolução de Equipamentos, Documentos e Informações

Na hipótese de desligamento da BlueOak, os Colaboradores não poderão reter ou portar consigo quaisquer equipamentos, ferramentas, documentos, arquivos e/ou Informações, incluindo cópias, gravações e/ou backups, mantidos em qualquer forma ou meio, por eles utilizados, produzidos e/ou acessados no exercício de suas respectivas funções, os quais são considerados, para todos os fins, de propriedade única e exclusiva da BlueOak.

Sem prejuízo do disposto acima, mediante solicitação da BlueOak ou conforme aplicável, os Colaboradores deverão, conforme o caso, destruir e/ou devolver à BlueOak equipamentos, ferramentas, documentos, arquivos e/ou Informações, incluindo cópias, gravações e/ou backups, mantidos em qualquer forma ou meio, por eles utilizados, produzidos e/ou acessados no exercício de suas respectivas funções na BlueOak.

Os Colaboradores deverão manter as Informações sob o mais absoluto sigilo mesmo na hipótese de desligamento, por qualquer motivo, da BlueOak. Na hipótese de utilização de ferramenta corporativa de Inteligência Artificial vinculada ao usuário, o acesso será imediatamente revogado por ocasião do desligamento.

14. Proteção e Controle

O Em complemento aos procedimentos previstos nesta Política, a BlueOak utiliza soluções de *firewall* e segurança de rede nos servidores para acesso à sua rede, visando à manutenção de um ambiente virtual de trabalho disponível e livre de vírus, bem como de acessos ou invasões indesejadas.

O sistema de prevenção a ataques de vírus será atualizado constantemente pelo DTI, de acordo com as melhores práticas adotadas pelo mercado.

Ademais, a BlueOak realiza regularmente o backup de arquivos e informações, mediante a utilização de unidade de disco externa ao servidor local, bem como de serviços de armazenamento de dados em nuvem (*cloud computing*).

A adoção de ferramentas de Inteligência Artificial pela BlueOak dependerá de avaliação prévia do DTI e do DRC quanto aos aspectos de segurança da informação, proteção de dados, confidencialidade, compliance e riscos operacionais.

Somente ferramentas aprovadas poderão ser utilizadas pelos Colaboradores no exercício de suas funções.

15. Incidente de Segurança da Informação e/ou Cibernético e Plano de Resposta

Os Colaboradores estão obrigados a reportar imediatamente ao Diretor de Compliance e PLD/FTP qualquer incidente envolvendo segurança da informação e/ou cibernético do qual tenham conhecimento, inclusive, mas não se limitando, a ocorrência de qualquer vazamento de Informações, ainda que oriundo de ação involuntária.

Em caso de incidentes envolvendo segurança da informação e/ou cibernéticos, o Diretor de Compliance e PLD/FTP, em conjunto com o DTI, adotará as medidas cabíveis de acordo com a gravidade de cada incidente e em observância à legislação e regulamentação aplicáveis, assim como às melhores práticas adotadas pelo mercado, observado que, na hipótese de vazamento de Informações, o Diretor de Compliance e PLD/FTP deverá comunicar o ocorrido (i) às partes interessadas e, quando aplicável, às autoridades regulatórias competentes; e (ii) quando caracterizada a ocorrência de incidente de segurança envolvendo Dado Pessoal ou Dado Pessoal Sensível que possa acarretar risco ou dano relevante aos titulares; e (ii) em se tratando de Dado Pessoal ou Dado Pessoal Sensível, à Autoridade Nacional de Proteção de Dados – ANPD em observância aos parâmetros exigidos pela Lei nº 13.709, de agosto de 2018, conforme alterada (“LGPD”). Para fins do item (ii) deste parágrafo, nos termos da LGPD, entende-se por “Dado Pessoal” a informação relacionada à pessoa natural identificada ou identificável, e “Dado Pessoal Sensível” o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Adicionalmente ao disposto acima, o Diretor de Compliance e PLD/FTP, em conjunto com o DTI, deverá adotar de imediato as medidas cabíveis com o objetivo de identificar e avaliar a causa do incidente de segurança da informação e/ou cibernético e extensão dos respectivos danos e prejuízos dele oriundos, incluindo a elaboração de um plano de ação, contemplando, dentre outras coisas, as medidas necessárias à rápida e efetiva solução das falhas e problemas identificados, de modo a possibilitar que as atividades voltem a ser executadas com segurança.

Constitui incidente de segurança, para fins desta Política, a inserção de Informações Confidenciais ou Privilegiadas em ferramenta de Inteligência Artificial não autorizada pela BlueOak.

Os Colaboradores poderão ser responsabilizados por violações às disposições desta Política, sujeitando-se à aplicação das medidas disciplinares cabíveis previstas no Código de Ética e Conduta da BlueOak, sem prejuízo de outras penalidades previstas na legislação aplicável.

O DRC deverá arquivar as documentações relacionadas aos incidentes envolvendo segurança da informação e/ou cibernéticos identificados, incluindo os respectivos planos de ação e medidas adotados.

16. Treinamentos

Os treinamentos referentes a esta Política serão conduzidos de acordo com o disposto no Código de Ética e Conduta da BlueOak

17. Canal de Comunicação

Eventuais dúvidas acerca desta Política poderão ser esclarecidas diretamente com o DTI ou ao DRC, conforme a natureza da consulta.

Anexo I à Política de Segurança da Informação e Cibernética da BlueOak Investments Asset Ltda.

**Termo de Adesão e Responsabilidade por Guarda e Uso de Equipamentos da
BlueOak Investments Asset Ltda**

Por meio deste Termo de Adesão e Responsabilidade por Guarda e Uso de Equipamentos da BlueOak Investments Asset Ltda. ("Política" e "BlueOak", respectivamente), declaro, de forma irrevogável e irretratável, que:

- (i) recebi, li e compreendi integralmente a Política, sendo que estou de acordo e adiro plenamente aos termos e condições da Política, comprometendo-me, neste ato, a cumprir todas as regras nela contidas;
- (ii) observarei e promoverei a observância da Política, enquanto perdurar o meu vínculo profissional com a BlueOak, comprometendo-me, ainda, a reportar qualquer violação à Política que seja do meu conhecimento;
- (iii) tenho ciência de que a violação das regras contidas na Política pode ensejar por parte da BlueOak medidas disciplinares, tais como advertência, desligamento e até responsabilização civil e criminal da minha pessoa, conforme legislação aplicável;
- (iv) tenho ciência de que os equipamentos, ferramentas e serviços a mim disponibilizados pela BlueOak para o exercício de minhas funções (em conjunto, "Equipamentos") são de propriedade exclusiva da BlueOak e de que somente poderei utilizar, no exercício de minhas atividades profissionais junto à BlueOak, ferramentas de Inteligência Artificial disponibilizadas, contratadas ou expressamente autorizadas pela BlueOak;
- (v) declaro que não vazarei quaisquer Informações Confidenciais, Informações Privilegiadas, dados pessoais, documentos internos, informações relativas aos Fundos BlueOak, investidores, clientes ou quaisquer outras informações relacionadas às atividades da BlueOak previamente compartilhadas com ferramentas de Inteligência Artificial, tampouco as usarei em prol de benefício pessoal e comprometo-me a não utilizar ferramentas de Inteligência Artificial pessoais ou não autorizadas pela BlueOak para tratar, armazenar, analisar, resumir, traduzir, compartilhar ou processar Informações Confidenciais, Informações Privilegiadas, dados pessoais, documentos internos, informações relativas aos Fundos BlueOak, investidores, clientes ou quaisquer outras informações relacionadas às atividades da BlueOak, ressalvada eventual situação previamente comunicada ao DRC;

- (vi) declaro estar de acordo com a política institucional da BlueOak de padronização das ferramentas de Inteligência Artificial utilizadas no ambiente de trabalho, comprometendo-me a utilizar exclusivamente as soluções corporativas disponibilizadas ou autorizadas pela BlueOak para fins relacionados às minhas atividades profissionais;
- (vii) atuarei com máximo zelo e diligência, para garantir a guarda e o uso adequados dos Equipamentos, em observância à Política, inclusive de forma a conservá-los em perfeito estado como se fossem de minha propriedade;
- (viii) informarei imediatamente à BlueOak, por meio do DRC e do DTI, qualquer dano, inutilização, extravio, roubo ou furto de Equipamentos;
- (ix) informarei imediatamente à BlueOak, por meio do DRC, qualquer incidente envolvendo segurança da informação e/ou cibernético do qual tenha conhecimento, incluindo o extravio, perda, roubo ou furto de documentos, arquivos e Informações, mantido em qualquer forma ou meio;
- (x) na hipótese de desligamento, por qualquer motivo, da BlueOak, devolverei à BlueOak os Equipamentos completos e em perfeito estado de conservação, assim como todo e qualquer documento, arquivo e Informação, mantido em minha posse por qualquer forma ou meio;
- (xi) estou ciente de que o descumprimento das regras relativas à utilização de ferramentas de Inteligência Artificial poderá caracterizar violação às políticas internas da BlueOak e ensejar a adoção das medidas disciplinares cabíveis, sem prejuízo das demais responsabilidades previstas na legislação aplicável; e
- (xii) estou ciente e concordo que, na hipótese de dano ou inutilização de qualquer Equipamento por uso inadequado, negligência ou imprudência, terei que restituir à BlueOak o valor do referido Equipamento ou, conforme o caso, de marca e modelo equivalentes ao Equipamento, de acordo com valor adotado pelo mercado para a aquisição de um novo.

São Paulo, _____ de _____ de _____.

Assinatura: _____

Nome: _____