Regras, Procedimentos e Controles Internos

Soho Capital Ltda.

Introdução

Este documento detalha as regras, procedimentos e controles internos da **Soho Capital Ltda.**, conforme exigido pelos artigos 15 e 17 da Resolução CVM nº 161/2022, o Código de Recursos de Terceiros e as diretrizes estabelecidas pela CVM e ANBIMA.

As diretrizes aqui apresentadas são aplicáveis a todos os sócios, diretores, administradores, empregados e colaboradores da EMPRESA, assegurando a conformidade com normas aplicáveis à coordenação de ofertas públicas de distribuição de valores mobiliários e mantendo os padrões éticos e profissionais requeridos.

1. Controles Internos

Os controles internos da Soho Capital são estruturados para garantir a integridade, precisão e confidencialidade das informações e assegurar o cumprimento permanente das normas aplicáveis.

Abaixo estão detalhadas as práticas de controle interno:

- Monitoramento Contínuo: Verificação contínua das conformidades das atividades de registro e coordenação de ofertas.
- Auditorias Internas: Realização de auditorias internas regulares para avaliar a eficácia dos controles e procedimentos estabelecidos.
- Relatórios Periódicos: Elaboração de relatórios de avaliação do cumprimento das normas e políticas, garantindo melhorias constantes nos processos de conformidade e segurança.

2. Política de Confidencialidade

A Política de Confidencialidade assegura que todas as informações relevantes e não públicas sejam rigorosamente controladas e acessadas apenas por pessoal autorizado:

- Acesso Restrito: Controle de acesso a informações sensíveis por meio de autenticação e autorização com base nas funções dos colaboradores.

- Acordo de Confidencialidade: Todos os colaboradores e parceiros assinam um termo de confidencialidade manual ou eletronicamente, em conformidade com o artigo 8o do Código de Recursos de Terceiros.
- Monitoramento e Revisão de Acesso: Monitoramento contínuo do acesso às informações e revisão periódica das políticas de confidencialidade.

3. Política de Segurança da Informação

Para proteger a integridade e segurança das informações armazenadas eletronicamente, a Soho

Capital adota uma política robusta de segurança da informação:

- Controles Avançados de Segurança: Implementação de firewalls, sistemas de detecção e prevenção de intrusões e criptografia de dados.
- Testes Periódicos de Segurança: Testes de vulnerabilidade e penetração são realizados semestralmente para identificar e corrigir falhas de segurança.
- Plano de Resposta a Incidentes: Estabelecimento de um plano de resposta a incidentes para mitigar os impactos de possíveis violações de segurança, com simulações de incidentes para garantir a pronta resposta dos colaboradores.

4. Programa de Treinamento

A política de treinamento da Soho Capital tem como objetivo capacitar seus colaboradores para o cumprimento das normas e o manuseio responsável das informações. O programa é composto por dois pilares: **Treinamento Inicial** e **Programa de Reciclagem Periódica**, com metodologias e conteúdos adaptados às funções específicas de cada colaborador.

4.1 Processo de Treinamento Inicial
O treinamento inicial é obrigatório para todos os novos colaboradores e cobre os seguintes tópicos:

1. **Princípios de Conformidade e Ética**:
    - Apresentação detalhada das normas de conduta e do Código de Ética da Soho Capital.
    - Reforço sobre responsabilidades legais e regulatórias, com base na Resolução CVM nº 161/2022.
2. **Segurança da Informação e Confidencialidade**:

- Orientações práticas sobre as políticas de segurança e confidencialidade da empresa.
- Uso de sistemas com acesso restrito e autenticação segura.

3. **Simulações e Estudos de Caso**:
    - Exercícios práticos para identificar e mitigar riscos operacionais, como vazamento de informações confidenciais.
4. **Treinamento Prático sobre Controles Internos**:
    - Instruções detalhadas sobre monitoramento, auditorias internas e relatórios periódicos de conformidade.
5. **Avaliação Final de Competência**:
    - Aplicação de testes de conhecimento e simulações para garantir a assimilação dos conteúdos apresentados.

4.2 Programa de Reciclagem Periódica
O programa de reciclagem é estruturado para manter a equipe atualizada sobre mudanças regulatórias e boas práticas do setor:

1. **Treinamento Semestral de Atualização**:
    - Apresentação de mudanças em normas regulatórias, diretrizes da CVM e políticas internas.
2. **Workshops Anuais sobre Ética e Conformidade**:
    - Palestras conduzidas por especialistas externos sobre práticas éticas e desafios do mercado financeiro.
3. **Simulações Periódicas de Incidentes**:
    - Exercícios práticos para testar a prontidão da equipe em situações de risco, como vazamentos de dados.
4. **Avaliações Trimestrais de Conhecimento**:
    - Aplicação de testes e relatórios individuais para identificar lacunas e propor medidas corretivas.
5. **Feedback Estruturado**:
    - Reuniões regulares para discutir a efetividade dos treinamentos e coletar sugestões para melhoria contínua.

5. Tratamento de Vazamento de Informações Confidenciais

Conforme o artigo 7º, parágrafo único, inciso II, do Código de Recursos de Terceiros, a Soho Capital estabelece procedimentos rigorosos para tratar casos de vazamento de informações confidenciais, reservadas ou privilegiadas, mesmo que oriundos de ações involuntárias:

1. **Identificação e Relato Imediato**:

- Qualquer colaborador que identificar ou suspeitar de um vazamento deve relatar imediatamente o incidente ao setor de Compliance por meio dos canais internos estabelecidos.

2. **Investigação e Análise do Incidente**:
    - O setor de Compliance iniciará uma investigação detalhada para determinar as causas, o impacto e a extensão do vazamento.
    - Será elaborado um relatório abrangente contendo as seguintes informações:
        - Natureza e origem do incidente.
        - Volume de informações comprometidas.
        - Potenciais implicações legais e regulatórias.
3. **Plano de Mitigação**:
    - Medidas corretivas serão implementadas imediatamente para mitigar os danos causados pelo incidente, incluindo:
        - Revogação de acessos não autorizados.
        - Correção de vulnerabilidades nos sistemas.
    - Se aplicável, as partes afetadas serão notificadas conforme previsto na legislação vigente.
4. **Revisão de Políticas e Treinamento Corretivo**:
    - Com base na análise do incidente, as políticas de segurança e confidencialidade serão revisadas para evitar recorrências.
    - Será realizado treinamento corretivo com a equipe, reforçando as diretrizes de segurança e as responsabilidades individuais.
5. **Documentação e Relatórios**:
    - Todos os detalhes do incidente, das medidas tomadas e dos resultados obtidos serão documentados em relatório oficial e arquivados para auditorias futuras.
    - O relatório será compartilhado com a administração e, se necessário, com autoridades reguladoras, conforme exigido pela legislação.
6. **Acompanhamento e Monitoramento Pós-Incidente**:
    - Após o incidente, o setor de Compliance realizará monitoramentos regulares para garantir que as medidas implementadas sejam eficazes.
    - Relatórios periódicos serão emitidos para avaliar o progresso e a segurança reforçada.

6. Regras de Restrição ao Uso de Sistemas, Acessos Remotos e Meios de Informação Confidencial

Conforme o artigo 7º, parágrafo único, inciso III, do Código de Recursos de Terceiros, a Soho Capital adota medidas específicas para garantir o uso controlado e seguro de sistemas, acessos remotos e quaisquer meios que contenham informações confidenciais, reservadas ou privilegiadas.

1. **Autenticação e Controle de Acesso**:
    - Todos os sistemas que armazenam ou processam informações confidenciais exigem autenticação multifatorial (MFA).
    - O acesso é restrito com base nas funções e responsabilidades dos colaboradores, sendo atualizado regularmente conforme mudanças nas atribuições.
2. **Monitoramento e Auditoria Contínuos**:
    - Todas as atividades de acesso aos sistemas são monitoradas e registradas por meio de ferramentas de auditoria interna.
    - Logs de acesso são revisados periodicamente para identificar comportamentos anômalos ou acessos não autorizados.
3. **Política de Dispositivos e Acessos Remotos**:
    - É permitido o uso de dispositivos apenas corporativos, com sistemas operacionais atualizados e aprovados pelo setor de TI.
    - Conexões remotas devem ser realizadas exclusivamente por meio de VPNs (Virtual Private Networks) seguras e monitoradas.
4. **Proibição de Armazenamento Local e Uso Não Autorizado**:
    - Informações confidenciais não podem ser armazenadas localmente em dispositivos pessoais.
    - É proibido o uso de e-mails pessoais, dispositivos não autorizados ou softwares de terceiros para o compartilhamento de informações confidenciais.
5. **Criptografia de Dados Sensíveis**:
    - Todos os dados classificados como confidenciais são criptografados durante o armazenamento e a transmissão.
    - Políticas de renovação e gestão de chaves criptográficas são aplicadas para proteger os dados.
6. **Treinamento e Conscientização**:
    - Colaboradores recebem treinamento regular sobre o uso seguro de sistemas e a importância de proteger informações sensíveis.
    - Simulações e exercícios práticos são conduzidos para reforçar a conscientização sobre ameaças de segurança digital.

7. **Penalidades para Violações**:
    - Qualquer violação das regras de restrição, incluindo tentativas de acessar sistemas sem autorização, será investigada pelo setor de Compliance.
    - Medidas disciplinares, que podem incluir demissão por justa causa, serão aplicadas em caso de violações intencionais ou negligência grave.
8. **Revisão Regular das Políticas**:
    - As regras de restrição são revisadas semestralmente para incorporar novas diretrizes regulatórias e práticas recomendadas de segurança.

7. Política de Segurança e Testes Periódicos de Sistemas de Informações Confidenciais

A Soho Capital adota uma política abrangente de segurança para proteger informações confidenciais, com foco especial nos sistemas mantidos em meio eletrônico. Essa política inclui testes periódicos de segurança para garantir a integridade, confidencialidade e disponibilidade das informações, aplicáveis a sócios, administradores, colaboradores e funcionários com acesso a esses sistemas.

1. **Objetivo dos Testes de Segurança**:
    - Identificar vulnerabilidades nos sistemas e processos que possam comprometer informações confidenciais.
    - Assegurar conformidade com as regulamentações da CVM e melhores práticas do setor de segurança da informação.
    - Proteger dados contra acessos não autorizados, ataques cibernéticos, perda ou destruição acidental.
2. **Abrangência dos Testes**:
   Os testes de segurança aplicam-se a todos os sistemas eletrônicos que armazenam ou processam informações confidenciais, incluindo:
    - Sistemas de gestão de carteiras de valores mobiliários.
    - Bancos de dados financeiros e administrativos.
    - Plataformas de comunicação interna e externa.
    - Dispositivos utilizados para acessar sistemas corporativos, como laptops, smartphones e servidores remotos.
3. **Tipos de Testes Realizados**:
    - **Testes de Vulnerabilidade**: Identificação de pontos fracos em aplicações, sistemas operacionais e dispositivos de rede.
    - **Testes de Penetração (Penetration Testing)**: Simulação de ataques cibernéticos para avaliar a resiliência dos sistemas contra tentativas de invasão.
    - **Revisões de Configuração**: Verificação de configurações de segurança, incluindo firewalls, permissões de acesso e criptografia.

- **Simulações de Engenharia Social**: Testes de conscientização com os profissionais, incluindo phishing simulado, para reforçar a segurança comportamental.

4. **Periodicidade dos Testes**:
   - **Semestralmente**: Testes de vulnerabilidade e penetração nos sistemas críticos.
   - **Trimestralmente**: Revisões de configuração de sistemas e dispositivos de rede.
   - **Anualmente**: Auditorias de segurança conduzidas por terceiros independentes para avaliar a eficácia geral das práticas de segurança.
5. **Responsáveis pela Execução dos Testes**:
   - **Setor de Tecnologia da Informação (TI)**: Responsável pela execução de testes internos e aplicação de correções.
   - **Auditores Externos**: Especialistas contratados para conduzir auditorias independentes e emitir relatórios detalhados.
   - **Setor de Compliance**: Monitora os resultados dos testes e garante a conformidade com as normas regulatórias.
6. **Gestão de Resultados e Planos de Ação**:
   - Vulnerabilidades críticas identificadas durante os testes são corrigidas imediatamente, com monitoramento contínuo até a resolução completa.
   - Relatórios de resultados são apresentados à alta administração e arquivados para auditorias futuras.
   - Planos de ação corretiva incluem atualizações de software, reforço de políticas de segurança e revisão de procedimentos internos.
7. **Treinamento e Conscientização**:
   - Após os testes, treinamentos específicos são realizados para reforçar a conscientização sobre práticas seguras e melhorias implementadas.
   - Simulações regulares são aplicadas para testar a prontidão dos sócios, administradores, colaboradores e funcionários.
8. **Revisão e Atualização da Política**:
   - A política de segurança e os procedimentos de teste são revisados anualmente para incorporar novas ameaças, avanços tecnológicos e mudanças no ambiente regulatório.

8. Assinatura de Termo de Confidencialidade

Conforme disposto no artigo 8º, parágrafo único, do Código de Recursos de Terceiros, a Soho Capital exige que todos os seus profissionais assinem, de forma manual ou eletrônica, um Termo de Confidencialidade abrangente, assegurando o sigilo sobre informações confidenciais,

reservadas ou privilegiadas às quais tenham acesso durante o exercício de suas atividades profissionais.

1. **Escopo do Termo de Confidencialidade**:
    - O termo cobre todas as informações consideradas confidenciais, incluindo, mas não se limitando a, dados de clientes, relatórios financeiros, estratégias de mercado, documentos internos e outras informações sensíveis.
    - Estabelece que o uso ou compartilhamento de tais informações é permitido apenas para fins autorizados e em conformidade com as normas legais e regulatórias vigentes.
2. **Modalidade de Assinatura**:
    - A assinatura pode ser feita manualmente em documento físico ou de forma eletrônica por meio de plataformas de assinatura digital, garantindo validade jurídica.
    - A coleta de assinaturas é realizada no momento da contratação e renovada anualmente como parte do processo de revisão de políticas internas.
3. **Obrigatoriedade e Prazos**:
    - Todos os profissionais, incluindo sócios, administradores, colaboradores e prestadores de serviço, são obrigados a assinar o Termo de Confidencialidade antes de iniciar suas atividades na instituição.
    - Em caso de mudanças nas políticas de confidencialidade, será solicitado que todos os envolvidos renovem o compromisso por meio de novo termo atualizado.
4. **Exceções Permitidas**:
    - O compartilhamento de informações confidenciais é permitido apenas nas seguintes situações:
        - Quando exigido por autoridades reguladoras, mediante autorização específica.
        - Conforme disposto em leis ou regulamentos aplicáveis.
    - Tais exceções devem ser registradas formalmente e submetidas à aprovação do setor de Compliance.
5. **Penalidades em Caso de Descumprimento**:
    - Qualquer violação do Termo de Confidencialidade será investigada pelo setor de Compliance, e ações disciplinares poderão incluir:
        - Advertências formais.
        - Rescisão contratual.
        - Ações judiciais para reparação de danos, se aplicável.
6. **Armazenamento e Registro**:

- Todos os Termos de Confidencialidade assinados são armazenados em repositório seguro, com acesso restrito ao setor de Compliance e à alta administração.
- A manutenção dos registros é feita por, no mínimo, cinco anos após o encerramento do vínculo profissional, em conformidade com a legislação vigente.

7. **Treinamento e Conscientização**:
    - Todos os profissionais são instruídos sobre os termos e condições do documento durante o processo de integração e nos treinamentos periódicos.

9. Regras de Acesso às Informações Confidenciais

Conforme disposto no artigo 7º, parágrafo único, inciso I, do Código de Recursos de Terceiros, a **Soho Capital Ltda.** estabelece regras rigorosas para o acesso e controle de informações confidenciais, reservadas ou privilegiadas. As diretrizes garantem que apenas pessoas autorizadas tenham acesso a essas informações, além de gerenciar adequadamente mudanças de função ou desligamento de profissionais.

1. **Controle de Acesso Baseado em Funções**
    - O acesso às informações confidenciais é restrito a sócios, administradores, colaboradores e funcionários cujas funções exijam o uso dessas informações.
    - O acesso é definido com base no princípio do "menor privilégio", garantindo que cada profissional tenha acesso apenas às informações necessárias para o desempenho de suas funções.
2. **Processo de Autorização**
    - O acesso é concedido após aprovação formal do setor de Compliance e registro em sistema interno de controle.
    - Profissionais recém-admitidos ou transferidos para novas funções recebem acesso apenas após:
        - Treinamento específico sobre confidencialidade e segurança.
        - Assinatura do Termo de Confidencialidade.
3. **Gestão de Acessos Não Autorizados**
    - Tentativas de acesso por pessoas não autorizadas são bloqueadas automaticamente por sistemas de segurança.
    - Incidentes são registrados e submetidos ao setor de Compliance, que realiza investigações e aplica medidas corretivas ou disciplinares, conforme a gravidade da ocorrência.
4. **Revisão Periódica de Acessos**

- O setor de Compliance realiza revisões semestrais para verificar se os níveis de acesso continuam adequados às funções exercidas pelos profissionais.
- Alterações nos níveis de acesso são comunicadas formalmente ao profissional e registradas no sistema.

5. **Gerenciamento de Mudanças de Função**
    - Quando há mudança de função dentro da instituição, os acessos são revisados imediatamente para garantir que estejam alinhados às novas responsabilidades.
    - Os acessos não mais necessários são revogados para evitar privilégios indevidos.
6. **Procedimentos de Desligamento**
    - No caso de desligamento de um profissional, o acesso às informações confidenciais é imediatamente suspenso assim que o setor de Recursos Humanos comunica o encerramento do vínculo.
    - O setor de TI realiza uma auditoria para verificar que nenhum dado foi transferido ou acessado indevidamente antes do desligamento.
    - O Termo de Confidencialidade assinado pelo profissional permanece válido após o desligamento, conforme as políticas internas e legislação aplicável.
7. **Treinamento e Conscientização**
    - Todos os profissionais recebem treinamento inicial e contínuo sobre as regras de acesso às informações confidenciais.
    - Simulações práticas são realizadas para garantir a compreensão e adesão às políticas de acesso.
8. **Documentação e Registro**
    - Todas as autorizações de acesso, revisões de níveis de acesso, alterações devido a mudanças de função e registros de desligamento são documentados e arquivados pelo setor de Compliance e TI.

10. Controles Internos para Atendimento às Normas, Políticas e Regulamentações Vigentes

Conforme o artigo 22 e os incisos I e II do artigo 23 da **Resolução CVM nº 21/21**, a **Soho Capital Ltda.** estabelece controles internos robustos que asseguram o atendimento permanente às normas, políticas e regulamentações aplicáveis às diversas modalidades de investimento, à atividade de administração de carteiras de valores mobiliários e aos padrões ético e profissional.

1. **Objetivo dos Controles Internos**
    - Garantir a conformidade com as regulamentações aplicáveis e as melhores práticas do mercado.

- Proteger a integridade das operações e assegurar que as decisões sejam tomadas com base em critérios técnicos e imparciais, alinhados aos melhores interesses dos clientes.

2. **Estrutura de Governança**
    - A governança da Soho Capital é estruturada para garantir a segregação de funções e a supervisão efetiva das atividades de administração de carteiras de valores mobiliários.
    - O **Comitê de Investimentos** e o **Comitê de Riscos** supervisionam as atividades, assegurando a conformidade com normas regulatórias e políticas internas.
3. **Controle de Modalidades de Investimento**
    - Todas as operações são avaliadas para garantir que estejam alinhadas com os perfis de risco e objetivos de investimento dos clientes.
    - Os processos incluem:
        - Seleção criteriosa de ativos e contrapartes.
        - Monitoramento contínuo da performance e da exposição ao risco.
4. **Segregação de Funções e Barreiras Informacionais**
    - Implementação de barreiras informacionais (Chinese Walls) para prevenir conflitos de interesse.
    - As funções relacionadas à gestão, execução e monitoramento de investimentos são segregadas para garantir a imparcialidade e a transparência.
5. **Avaliação de Riscos**
    - Utilização de sistemas integrados para identificar, mensurar, monitorar e mitigar riscos financeiros, operacionais e de compliance.
    - A avaliação contínua inclui a análise de riscos de mercado, liquidez e crédito.
6. **Monitoramento e Auditoria**
    - Auditorias internas trimestrais realizadas para avaliar a eficácia dos controles internos.
    - Revisões independentes conduzidas por auditores externos anualmente.
7. **Padrões Ético e Profissional**
    - Compromisso com os mais altos padrões de ética e conduta profissional, assegurados por meio de treinamentos regulares e monitoramento de práticas internas.
    - Políticas claras para identificar e mitigar conflitos de interesse, conforme disposto na Resolução CVM nº 21/21.
8. **Treinamento e Capacitação**

- Todos os sócios, diretores, administradores, empregados e colaboradores recebem treinamento regular sobre regulamentações, práticas éticas e políticas internas.
- Simulações e workshops são realizados periodicamente para reforçar o compromisso com a conformidade e a excelência profissional.

9. **Relatórios e Documentação**
    - Elaboração de relatórios periódicos que incluem:
        - Desempenho das carteiras.
        - Compliance com regulamentações.
        - Identificação e mitigação de riscos.
    - Os relatórios são compartilhados com a alta administração e arquivados para auditorias futuras.
10. **Supervisão e Revisão Periódica**
    - Os controles internos são revisados regularmente para garantir alinhamento com mudanças no ambiente regulatório e no mercado.
    - Melhorias contínuas são implementadas com base nas auditorias internas e externas.

11. Política de Identificação, Administração e Eliminação de Conflitos de Interesse

Conforme o inciso II do artigo 23 da Resolução CVM nº 21/21, a Soho Capital estabelece políticas específicas para identificar, administrar e eliminar eventuais conflitos de interesse que possam comprometer a imparcialidade das pessoas que desempenham funções relacionadas à administração de carteiras de valores mobiliários.

1. **Objetivo da Política de Conflitos de Interesse**:
    - Assegurar que todas as decisões relacionadas à administração de carteiras sejam tomadas no melhor interesse dos clientes, sem influência indevida de interesses pessoais, comerciais ou institucionais.
    - Prevenir situações que possam comprometer a imparcialidade ou gerar dúvidas sobre a integridade das operações.
2. **Identificação de Conflitos de Interesse**:
    - Realização de mapeamentos regulares para identificar potenciais conflitos em atividades como:
        - Negociação de valores mobiliários.
        - Contratação de serviços de terceiros.
        - Relacionamento com clientes ou partes relacionadas.

- Uso de questionários obrigatórios para colaboradores declararem interesses pessoais ou comerciais que possam interferir em suas responsabilidades.

3. **Administração de Conflitos de Interesse**:
    - Implementação de barreiras informacionais (Chinese Walls) para restringir o fluxo de informações entre áreas que possam gerar conflitos.
    - Adoção de procedimentos específicos para evitar a priorização de interesses próprios ou de partes relacionadas em detrimento dos clientes.
    - Definição de critérios objetivos para a seleção de ativos, serviços ou contrapartes, com base em análises imparciais e alinhadas ao mandato de investimento.
4. **Eliminação de Conflitos de Interesse**:
    - Medidas corretivas imediatas para resolver situações de conflito identificadas, incluindo a exclusão de indivíduos potencialmente comprometidos de processos de tomada de decisão.
    - Alterações em processos operacionais e na estrutura organizacional, quando necessário, para mitigar riscos de conflito de interesse recorrente.
5. **Procedimentos Internos de Monitoramento**:
    - Monitoramento contínuo por meio do setor de Compliance para identificar e registrar eventuais conflitos emergentes.
    - Revisões periódicas das políticas de conflito de interesse para incorporar mudanças regulatórias ou estruturais.
6. **Treinamento e Conscientização**:
    - Todos os colaboradores recebem treinamentos específicos para reconhecer e relatar situações de conflito de interesse.
    - Simulações e estudos de caso são aplicados para reforçar a conscientização e promover a adoção de práticas éticas.
7. **Declaração de Conflitos**:
    - É obrigatória a declaração formal de potenciais conflitos de interesse por parte de colaboradores, administradores e sócios, com revisões anuais e sempre que houver mudanças em suas circunstâncias pessoais ou profissionais.
    - As declarações são registradas e revisadas pelo setor de Compliance, que decide sobre ações corretivas, quando aplicável.
8. **Gestão de Consequências**:
    - Em caso de descumprimento das políticas de conflito de interesse, sanções podem incluir advertências formais, medidas disciplinares ou rescisão contratual.

- Incidentes significativos são reportados à alta administração e, quando necessário, às autoridades reguladoras competentes.

9. **Supervisão e Governança**:
    - O Comitê de Risco é responsável por revisar casos críticos de conflitos de interesse e monitorar as medidas adotadas para sua mitigação.
    - Relatórios regulares sobre a gestão de conflitos são apresentados ao Comitê de Compliance e à alta administração.
10. **Revisão e Atualização da Política**:
    - A política de conflitos de interesse é revisada anualmente para assegurar sua eficácia e conformidade com normas regulatórias.

TERMO DE CONFIDENCIALIDADE

Soho Capital Ltda.
Identificação
Este Termo de Confidencialidade é firmado entre a Soho Capital Ltda., inscrita no CNPJ nº [inserir], com sede em [endereço], doravante denominada "EMPRESA", e [NOME COMPLETO], portador do CPF nº [inserir], residente em [endereço], doravante denominado "PROFISSIONAL".

1. Objetivo
O presente termo tem como objetivo garantir a proteção e o sigilo de todas as informações confidenciais, reservadas ou privilegiadas às quais o PROFISSIONAL tenha acesso durante o exercício de suas atividades profissionais na EMPRESA, conforme as políticas internas, as regulamentações da CVM e demais legislações aplicáveis.

---

2. Definição de Informações Confidenciais
Para os fins deste termo, considera-se como "Informações Confidenciais" qualquer dado, documento, estratégia, sistema, processo, plano de negócio, relatórios financeiros ou quaisquer outros materiais que:

- Não sejam de domínio público.
- Estejam protegidos por normas regulatórias ou contratuais.
- Estejam relacionados a clientes, parceiros, fornecedores ou colaboradores da EMPRESA.

---

3. Obrigações do PROFISSIONAL
O PROFISSIONAL compromete-se a:

1. Manter absoluto sigilo sobre todas as Informações Confidenciais a que tiver acesso, utilizando-as apenas para a execução de suas atividades profissionais.
2. Não reproduzir, copiar, transmitir, compartilhar ou divulgar quaisquer Informações Confidenciais sem autorização expressa da EMPRESA.

3. Proteger as Informações Confidenciais contra acessos não autorizados, perda, roubo ou uso indevido.
4. Comunicar imediatamente ao setor de Compliance qualquer incidente que possa comprometer a confidencialidade das informações.
5. Respeitar as regras de acesso a sistemas e dados conforme as políticas internas da EMPRESA, utilizando apenas dispositivos e canais autorizados.

---

4. Regras para Uso de Sistemas e Acessos
O PROFISSIONAL concorda em utilizar apenas os sistemas e acessos fornecidos pela EMPRESA, comprometendo-se a:

1. Respeitar os níveis de acesso definidos com base em suas funções.
2. Utilizar autenticação multifatorial e ferramentas de segurança aprovadas pela EMPRESA.
3. Não armazenar informações confidenciais em dispositivos pessoais ou plataformas não autorizadas.
4. Encerrar imediatamente todos os acessos à EMPRESA em caso de mudança de função ou desligamento.

---

5. Validade do Termo
Este termo permanece válido durante todo o vínculo contratual entre o PROFISSIONAL e a EMPRESA e continua em vigor por cinco (5) anos após o encerramento do vínculo, exceto quando a legislação aplicável determinar prazo superior.

---

6. Penalidades por Descumprimento
O descumprimento das obrigações previstas neste termo poderá resultar em:

1. Abertura de processo disciplinar, que pode incluir advertências formais ou rescisão contratual por justa causa.
2. Responsabilização civil e criminal, caso sejam constatados danos à EMPRESA ou a terceiros.
3. Comunicação de incidentes às autoridades regulatórias, conforme exigido pela legislação.

---

7. Exceções Permitidas
As obrigações previstas neste termo não se aplicam a informações que:

1. Sejam de domínio público na data de assinatura deste termo.
2. Tornem-se de domínio público por meios legais, sem violação das obrigações aqui estabelecidas.

3. Sejam divulgadas mediante ordem judicial ou regulamentação aplicável, desde que o PROFISSIONAL notifique a EMPRESA previamente.

---

8. Declaração do PROFISSIONAL
Ao assinar este termo, o PROFISSIONAL declara ter ciência de todas as políticas e regras de confidencialidade da EMPRESA, conforme previsto nos **Regras e Procedimentos de Deveres Básicos do Código de Recursos de Terceiros**, na **Resolução CVM nº 21/21**, e nas demais regulamentações aplicáveis.

---

9. Disposições Gerais

1. O PROFISSIONAL declara que participou do treinamento inicial e das reciclagens periódicas sobre confidencialidade e segurança da informação promovidos pela EMPRESA.
2. Este termo será arquivado digitalmente e fisicamente no setor de Compliance, podendo ser acessado apenas por pessoal autorizado.
3. Eventuais alterações neste termo serão comunicadas por escrito ao PROFISSIONAL, que deverá assiná-las para manter sua validade.

---

10. Assinatura

Assinatura da EMPRESA
Nome: _____
Cargo: _____
Data: _____

Assinatura do PROFISSIONAL
Nome: _____
CPF: _____
Data: _____