ICON CAPITAL
Gestão de Investimentos

POLÍTICA DE CONTROLES INTERNOS

Elaboração	Versão
03/2024	1.0
03/2025	1.1

Índice

1. OBJETIVO

Esta Política de Controles Internos (“Política”) foi desenvolvida pela Icon Capital (“Gestora”) em conformidade com a Resolução CVM 21/2021, com o objetivo de assegurar a contínua aderência às normas, políticas e regulamentações aplicáveis à administração de carteiras de valores mobiliários.

A responsabilidade pela implementação e supervisão desta Política recai sobre a Diretoria da Gestora, com o suporte da Área de Compliance.

Todos os profissionais vinculados à Gestora, incluindo sócios, colaboradores e contratados, têm a responsabilidade de compreender e seguir as normas e procedimentos estabelecidos. Qualquer violação desta Política resultará em medidas disciplinares apropriadas, que podem incluir advertências, suspensões e rescisões contratuais.

Reconhecendo a importância de um sistema de controle interno eficaz, a Gestora busca garantir a integridade das informações financeiras, mitigar riscos, cumprir as exigências legais, regulatórias.

2. VERIFICAÇÃO E CUMPRIMENTO DE POLÍTICAS INTERNAS

A responsabilidade pela revisão e cumprimento da Política cabe ao Diretor de Compliance, Risco e PLD-FT, conforme estipulado pela Resolução CVM 21/2021. Este Diretor possui plena autonomia e independência, reportando-se diretamente ao Comitê de Compliance.

As responsabilidades do Diretor de Compliance, Risco e PLD-FT englobam uma série de atividades essenciais. Isso inclui, mas não se limita a:

- Responder prontamente às solicitações de todos os Colaboradores;
- Realizar monitoramento contínuo da eficácia dos controles internos;
- Garantir a conformidade com o Código de Ética;
- Identificar possíveis violações das políticas, do Código de Ética e de outras normas da empresa;
- Prestar assessoria à gestão dos negócios na compreensão, interpretação e impacto da legislação;

- Disseminar o Código de Ética e as Políticas da empresa entre os Colaboradores e stakeholders;
- Monitorar o cumprimento das alocações em ativos estabelecidas pelo Comitê de Gestão de Recursos para os veículos de investimento sob gestão; e
- Controlar a documentação pendente dos veículos de investimento e dos ativos em que estes investem.

Ao menos uma vez por ano, a área de Compliance deve conduzir uma revisão completa da Política, da agenda regulatória, do programa de treinamento (incluindo a Diretoria de Compliance, Risco e PLD-FT), dos formulários e testes de aderência. Como resultado da revisão anual, a área de Compliance deve elaborar um relatório de conclusões de controles internos, conforme disposto no artigo 25 da Resolução CVM 21/2021.

3. POLÍTICAS DE CONFIDENCIALIDADE

A confidencialidade é um princípio fundamental na Gestora, especialmente para informações não públicas. Todos os colaboradores, ao ingressarem na empresa, assinam uma Declaração de Conformidade com o Código de Ética da Icon Capital, comprometendo-se a manter sob sigilo absoluto todas as informações confidenciais a que tiverem acesso.

A tipificação e as orientações detalhadas sobre como acessar, manusear, arquivar e proteger as informações confidenciais estão descritas no item 6 do Código de Ética, Segurança da Confidencialidade e Sigilo das Informações. A Diretoria de Compliance é responsável por verificar anualmente o conhecimento e o compromisso dos colaboradores com as políticas e manuais de controles internos.

A Diretoria de Compliance também é responsável por manter treinamento para todos os colaboradores e acompanhamento especial para aqueles que acessam informações confidenciais, reservadas ou privilegiadas e participam do processo de decisão de investimento.

Os exames destinados a avaliar a entrada dos funcionários, particularmente aos dados digitais, devem assegurar a devida confidencialidade e controle sobre os dados sensíveis, garantir a integridade dos recursos computacionais contra quaisquer modificações indevidas e facilitar a execução de auditorias e vistorias.

Os detentores de informações confidenciais são identificados pelo controle de acesso aos sistemas de informação de cada departamento. Cada colaborador possui login e senha pessoais e intransferíveis, permitindo a rastreabilidade em caso de vazamento.

O acesso aos sistemas é liberado com base no princípio da necessidade da informação para a função do colaborador. O controle é feito por perfis de acesso que segregam as funções das diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gestora possui controles internos para que o acesso seja liberado mediante aprovação da área de Compliance.

Qualquer suspeita de vazamento de informações confidenciais, reservadas ou privilegiadas deve ser imediatamente reportada ao Diretor de Compliance da Gestora. O Departamento de Compliance conduzirá uma investigação interna para determinar se houve vazamento, identificar os responsáveis e a extensão do dano.

Se confirmado o vazamento, a Gestora tomará as medidas necessárias para minimizar os danos causados, incluindo notificação imediata aos clientes afetados, revisão dos procedimentos internos, comunicação às autoridades, se necessário e adoção de medidas disciplinares, incluindo demissão e ações legais, contra os envolvidos.

A Gestora se compromete a proteger as informações confidenciais de seus clientes e a tomar todas as medidas necessárias para evitar vazamentos. A adoção de controles rigorosos de segurança, treinamento de funcionários e a implementação de políticas claras de segurança da informação são fundamentais para garantir a proteção dos dados dos clientes.

4. POLÍTICAS DE SEGURANÇA

A Política de Segurança da Informação é um conjunto contínuo de medidas destinadas a proteger os ativos de informação da empresa, contribuindo para alcançar sua missão e objetivos.

As informações são acessíveis apenas por indivíduos autorizados, sendo mantidas intactas e protegidas contra alterações indevidas, sejam acidentais ou intencionais. O detalhamento das restrições de acesso e uso de sistemas remotos está contemplado no item 4.1, a seguir.

Cada colaborador é plenamente responsável pela posse e uso adequado de suas credenciais de acesso aos sistemas, como logins e senhas, bem como pelas atividades resultantes desse uso. O compartilhamento de credenciais é estritamente proibido em todas as circunstâncias.

O monitoramento abrangente das atividades dos colaboradores na Gestora e no mercado de capitais tem como objetivo dissuadir qualquer tentativa de uso de informações confidenciais para benefício próprio ou de terceiros.

Os Diretores da empresa têm acesso a todos os e-mails, documentos recebidos e enviados, conforme estipulado nos itens sobre Monitoramento de Correio Eletrônico e Uso de Computadores e Acesso à Internet.

Na rede da Gestora, os sócios e funcionários têm acesso exclusivo aos diretórios de suas áreas e alçadas, conforme política Zero Trust. Apenas os Diretores têm acesso a todos os diretórios da rede. Se um colaborador precisar de acesso a informações confidenciais e de acesso restrito, elas só poderão ser fornecidas ou divulgadas com autorização prévia e justificada da Diretoria.

A utilização de recursos de rede, sistemas e outras fontes de informação é monitorada pela Gestora por meio de registros de auditoria em telefonia, computadores, sistemas, mensagens eletrônicas, acessos à internet, entre outros. Essas informações podem ser coletadas e usadas, a critério da empresa, para a realização de investigações internas ou para cumprir medidas judiciais, sem aviso prévio às pessoas envolvidas, mas sempre respeitando a privacidade dos colaboradores. Todos os proprietários e usuários, bem como todos os acessos e tentativas de acesso, ficam registrados nos sistemas. É importante ressaltar que todos os ramais de telefonia da Gestora são gravados, o que possibilita a identificação de qualquer uso indevido.

Sob a responsabilidade do Diretor de Compliance, Risco e PLD-FT, a Icon Capital realiza anualmente diversos testes para monitorar e proteger seus sistemas e dados contra acessos não autorizados, violações e falhas.

A tabela abaixo apresenta os testes realizados e seus objetivos:

Medida	Objetivo
Verificação do login de todos os colaboradores aos sistemas de informação e níveis de acesso a informações confidenciais	Detectar acessos não autorizados e garantir que os colaboradores possuem apenas os acessos necessários.
Alteração de senha de acesso dos colaboradores	Garantir a segurança das contas dos colaboradores.
Testes no firewall	Detectar e prevenir ataques externos.
Manutenção preventiva de hardware por empresa contratada de tecnologia da informação	Garantir o bom funcionamento dos sistemas e prevenir falhas.
Atualização de software, quando aplicável, pela empresa contratada de tecnologia da informação	Corrigir vulnerabilidades de segurança e garantir o bom funcionamento dos sistemas.
Testes no backup (salvamento de informações) realizado na nuvem e de integridade do hardware com cópia local	Garantir que as informações da empresa estejam seguras e protegidas contra perda ou corrupção.

A Gestora está comprometida com a segurança da informação e investe continuamente em medidas para proteger seus dados e sistemas. A seguir são detalhadas as restrições ao uso de sistemas e regras para acesso remoto.

4.1 RESTRIÇÃO AO USO DE SISTEMAS E ACESSO REMOTO

Para garantir a segurança e a confidencialidade das informações, a Gestora adota as seguintes medidas de controle no uso de sistemas e acessos remotos:

1. Restrição de Acesso: Acesso a sistemas que contêm informações confidenciais, reservadas ou privilegiadas será estritamente limitado a usuários autorizados, conforme suas funções e responsabilidades. A autorização será concedida pelo departamento de TI, em conjunto com o departamento de compliance, e será revisada periodicamente.

2. Autenticação 2fa: O acesso remoto aos sistemas da empresa, principalmente e-mails e login nos diretórios compartilhados pelo OneDrive, deve ser realizado por meio de autenticação de dois fatores, garantindo que apenas usuários autorizados possam acessar informações sensíveis de locais remotos.

3. Registro de Atividades: Todas as atividades realizadas nos sistemas que envolvem informações confidenciais serão registradas e monitoradas. Logs de acesso e alterações serão revisados regularmente para detectar e responder a atividades suspeitas.

4. Treinamento de Segurança: Todos os sócios, diretores, membros da alta administração e profissionais com acesso a informações confidenciais participarão regularmente de treinamentos focados na segurança da informação e no cumprimento das políticas de acesso.

5. Uso de Dispositivos Seguros: O acesso remoto só será permitido por meio de dispositivos que atendam aos padrões de segurança estabelecidos pela Icon Capital. Tais dispositivos deverão estar equipados com software de segurança atualizado e configurações aprovadas pelo departamento de TI.

6. Política de Zero Trust: Implementação do modelo de segurança Zero Trust, onde não se presume confiança apenas pelo fato do acesso originar-se de dentro da rede corporativa. Verificações de segurança são necessárias para cada tentativa de acesso a recursos críticos, independentemente da origem do acesso. O acesso aos recursos do sistema nunca deverá ser franqueado de maneira total, mas sempre limitado à necessidade do usuário.

7. Violações e Sanções: Qualquer violação das políticas de uso de sistemas e acesso remoto resultará em ações corretivas e, dependendo da gravidade, sanções disciplinares.

Essas medidas são fundamentais para manter a integridade e a segurança das informações confidenciais, reservadas ou privilegiadas da Gestora e para cumprir as disposições legais e regulatórias aplicáveis.

5. POLÍTICA DE TREINAMENTO

A Gestora possui um programa de treinamento abrangente para todos os colaboradores, com o objetivo de garantir o cumprimento das normas legais e regulamentares, manter um elevado padrão de prestação de serviços e promover uma cultura ética na empresa.

Ao ingressar na Gestora, todos os colaboradores participam de um treinamento abrangente com o objetivo de integrá-los à cultura da organização e garantir o conhecimento das normas e políticas que regem suas atividades.

O treinamento aborda as atividades da Gestora, seus produtos, serviços, mercado de atuação, as normas e políticas internas da empresa, as principais leis e normas que regulam o setor em que a empresa atua, buscando garantir que os colaboradores estejam em conformidade com as obrigações legais.

Este treinamento inicial é fundamental para que os novos colaboradores se familiarizem com a cultura da Gestora e assumam suas funções com responsabilidade e conhecimento.

A Gestora oferece um programa de treinamento contínuo para todos os colaboradores. Este programa visa manter os colaboradores atualizados sobre as mudanças nas leis e normas, as novas políticas da empresa, melhores práticas de compliance, riscos e como evitá-los.

É responsabilidade do Diretor de Compliance conduzir o programa de treinamento e garantir que todos os colaboradores estejam treinados de acordo com as necessidades da empresa. Os colaboradores são responsáveis por participar de todos os treinamentos e manter-se atualizados sobre as normas e políticas da empresa.

O Diretor de Compliance é responsável por controlar a participação dos colaboradores nos treinamentos e avaliar a efetividade do programa e o Comitê de Compliance pode contratar profissionais especializados para conduzir treinamentos específicos, quando necessário.

A participação nos treinamentos é obrigatória para todos os colaboradores. A assiduidade e a dedicação aos treinamentos são essenciais para garantir o cumprimento das normas e políticas da empresa.

6. INVESTIMENTOS PESSOAIS, PRESENTES E *SOFT DOLLAR*

Os colaboradores da Gestora devem verificar anualmente se seus investimentos pessoais estão em conformidade com a Política Interna de Compra e Venda de Valores Mobiliários.

Os colaboradores podem aceitar presentes, materiais, benefícios, cursos, viagens ou outras vantagens com valor não superior a R$ 400,00 (quatrocentos reais.

Benefícios econômicos de caráter não pecuniário também podem ser aceitos, desde que sejam compatíveis com o tamanho e a posição do relacionamento com o fornecedor, possam ser revertidos para a melhoria dos serviços prestados aos clientes, não comprometam a independência da gestão, não ensejem exclusividade ou volumes mínimos de negociação com prestadores de serviços e não violem o código de ética da Gestora.

Ao avaliar se um benefício econômico oferecido por fornecedores é excessivo, o colaborador deverá verificar se a natureza do benefício é típica do tamanho e da posição do relacionamento com o cliente ou fornecedor.

A pertinência de qualquer benefício econômico deve ser discutida com o Diretor de Compliance, Riscos e PLD-FT.

7. SISTEMA DE COMPLIANCE

Em linha com as diretrizes de conformidade, a Icon Capital adota o sistema Compliasset para conduzir uma supervisão qualitativa eficaz. Esse sistema possibilita a organização de rotinas, agendamentos, atribuição de responsabilidades e estabelecimento de prazos para o cumprimento das tarefas relacionadas à conformidade regulatória e normativa.

Essa ferramenta desempenha um papel crucial na garantia de que os investimentos estejam em conformidade com as diretrizes estabelecidas, oferecendo transparência e segurança nas operações financeiras.

8. DISPOSIÇÕES GERAIS

Esta Política aplica-se a todas as áreas e colaboradores da Gestora envolvidos na seleção e alocação de ativos dos Fundos, devendo ser observada em conjunto com a legislação e regulamentação aplicáveis.

Em caso de conflito entre o disposto nesta Política e normas legais ou regulamentares, prevalecerão as últimas. O descumprimento das diretrizes aqui estabelecidas sujeitará os responsáveis às sanções previstas nas políticas internas e na legislação em vigor.

A revisão de parâmetros e premissas referentes ao teor deste documento, bem como dos demais manuais e políticas, deve ocorrer em periodicidade anual ou mediante demanda, sendo de responsabilidade do Diretor de Compliance.

9. MANUTENÇÃO DOS ARQUIVOS

A revisão de parâmetros e premissas referentes ao teor deste documento, bem como dos demais manuais e políticas, deve ocorrer em periodicidade anual ou mediante demanda, sendo de responsabilidade do Diretor de Compliance.

Todos os documentos utilizados ou gerados para a sua manutenção deverão permanecer arquivados, em meio eletrônico ou físico, pelo prazo mínimo de 5 (cinco) anos, em conformidade com a recomendação expedida pelos órgãos regulatórios e com as políticas internas da Icon Capital.

ANEXO A - Termo de Confidencialidade da Icon Capital

Eu, [**Nome do Colaborador**], CPF **xxx.xxx.xxx-xx**, declaro ter lido e compreendido os termos de confidencialidade da Icon Capital. Ao assinar este documento, confirmo que estou ciente e concordo com todas as suas cláusulas.

1. Informações Confidenciais: Toda informação, oral ou escrita, transmitida pela Icon Capital ao colaborador em razão de suas funções, é considerada confidencial e de propriedade da empresa. Isso inclui, mas não se limita a: i) informações técnicas, operacionais, comerciais e jurídicas; ii) know-how, planos de negócios, métodos de contabilidade; iii) técnicas e experiências acumuladas, documentos, contratos, papéis, e; iv) estudos, pareceres, pesquisas e fórmulas.

2. Responsabilidades do Colaborador: O colaborador que recebe informação confidencial se obriga a: i) Não discuti-la com terceiros, usá-la, divulgá-la, revelá-la ou cedê-la a qualquer título; ii) Adotar cautelas e precauções para impedir seu uso indevido; iii) Responsabilizar-se por impedir a divulgação ou a utilização das informações confidenciais; iv) Restituir imediatamente à empresa qualquer documento ou suporte que contenha as informações confidenciais, sempre que solicitado ou quando as informações deixarem de ser necessárias.

3. Violação: O colaborador que violar qualquer cláusula deste Termo estará sujeito a sanções e penalidades legais.

4. Prazo: As obrigações de confidencialidade, responsabilidades e outras obrigações derivadas deste Termo vigorarão durante todo o contrato de trabalho e por 2 (dois) anos após o desligamento do colaborador da Icon Capital.

5. Tipo de Acesso ao Diretório: O colaborador deve indicar se o seu acesso ao diretório da empresa é restrito ou irrestrito.

Goiânia, _____ de _____ de _____

_____

Assinatura do Colaborador