

REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

PONTAL CAPITAL GESTORA DE RECURSOS LTDA.

Setembro/2025 – Versão 1.0

ÍNDICE

INTRODUÇÃO.....	3
ABRANGÊNCIA.....	3
PRINCÍPIOS NORTEADORES.....	3
DIRETRIZES	4
RESPONSABILIDADES	4
MATERIAL PUBLICITÁRIO	6
CONFLITOS DE INTERESSE	7
CONFLITOS DE INTERESSE – ACORDO DE REMUNERAÇÃO	7
SEGREGAÇÃO DAS ATIVIDADES.....	8
INFORMAÇÕES CONFIDENCIAIS.....	8
PROGRAMA DE SEGURANÇA DA PONTAL CAPITAL	12
DISPOSIÇÕES GERAIS.....	23
VIGÊNCIA E ATUALIZAÇÃO	24
ANEXO I - TERMO DE ADESÃO À POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS, E SEGURANÇA CIBERNÉTICA DA PONTAL CAPITAL GESTORA DE RECURSOS LTDA.....	25

INTRODUÇÃO

Estas Regras, Procedimentos e Descrição dos Controles Internos (“Política”) têm por objetivo estabelecer regras e procedimentos, bem como descrever os controles internos a serem implementados e observados no desempenho das atividades da PONTAL CAPITAL GESTORA DE RECURSOS LTDA. (“Gestora” ou “Pontal Capital”).

As regras e procedimentos aqui previstos visam garantir o atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de Gestão e aos padrões ético e profissional.

Dessa forma, objetivam facilitar a identificação de eventos, reduzir a frequência de surgimento de eventos, e mitigar riscos decorrentes de eventos quando estes surgirem, bem como, disseminar a cultura de controles para garantir o cumprimento das normas contidas na Resolução CVM n.º 21, de 25 de fevereiro de 2021 (“Resolução CVM n.º 21/2021”), no Código ANBIMA de Administração e Gestão de Recursos de Terceiros (“Código AGRT”) e nas demais normas estabelecidas pelos órgãos reguladores e autorreguladores.

Sem prejuízo de quaisquer disposições desta Política, a Gestora também observará, conforme aplicável, eventuais políticas de controle interno de seu grupo de controle internacional, de modo a estabelecer ainda mais robustez operacional nas atividades da Gestora.

ABRANGÊNCIA

Esta Política aplica-se a todos os Colaboradores da Gestora.

PRINCÍPIOS NORTEADORES

As atividades de controle devem ser avaliadas com frequência razoável, tomando como referência as boas práticas de governança corporativa.

Controles internos consistem em um ou mais processos desenvolvidos para garantir o atingimento dos objetivos da Gestora, com relação à:

- a) Eficiência e efetividade operacional;

- b) Confiança nos registros de dados e informações;
- c) Conformidade; e
- d) Abordagem baseada em gestão de risco.

DIRETRIZES

Esta Política tem como diretrizes:

- a) Disseminar a cultura sobre a importância dos controles internos a todos os Colaboradores da Gestora;
- b) Assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;
- c) Alinhar a estrutura dos controles internos aos objetivos do negócio e aos riscos deles decorrentes;
- d) Criar o arcabouço necessário para a existência de atribuição de responsabilidades e delegação de autoridade, observada a estrutura hierárquica da Gestora;
- e) Possibilitar a elaboração de relatórios sobre a situação dos controles internos;
- f) Estabelecer os fluxos de aprovação mediante alçadas; e
- g) Assegurar a revisão periódica dos processos de controles internos.

RESPONSABILIDADES

A. Implementação e Manutenção de Processos de Controles Internos:

Os gestores de cada uma das áreas da Gestora são responsáveis por estabelecer, manter, promover e avaliar as atividades desempenhadas e estabelecer controles internos adequados e eficazes, bem como documentá-los de maneira clara e objetiva.

A Área de *Compliance* deverá receber de cada um dos gestores de área relatório compreendendo status dos controles internos por eles implantados, incluindo os eventos negativos e impactos. De posse dos relatórios, o Sr. Carlos Jose Lancellotti Narciso, inscrito no CPF/MF sob o nº 680.864.667-87, diretor responsável pelas atividades de risco, compliance e prevenção à lavagem de dinheiro da Gestora (“Diretor de Compliance, Risco e PLD”), emitirá relatório com eventuais propostas para os Administradores da Gestora.

A Gestora estabeleceu políticas apartadas com o propósito de consolidar princípios e regras sobre as seguintes matérias:

- Ética e Conduta;
- Confidencialidade;
- Investimentos Pessoais;
- *Know Your Client* (KYC) e Prevenção à Lavagem de Dinheiro (PLD);
- Combate à Corrupção;
- Treinamento e Reciclagem de Colaboradores;
- Rateio e Divisão de Ordens;
- Gestão de Riscos;
- Exercício de Voto;
- Contratação de Terceiros;
- Segurança Cibernética e de Informações;
- Continuidade de Negócios;
- Seleção e Alocação de Ativos;
- Certificação Continuada.

B. Análise dos Processos de Controles Internos:

O Diretor de Compliance, Risco e PLD é o encarregado pela definição dos métodos de avaliação e monitoramento dos processos de controles internos da Gestora, sendo também o principal responsável pelo atendimento aos órgãos reguladores e autorreguladores.

C. Avaliação dos Processos de Controles Internos:

O Diretor de Compliance, Risco e PLD é responsável por promover a avaliação independente das atividades desenvolvidas pelas diversas áreas da Gestora, de modo a aferir a adequação dos controles estabelecidos ao cumprimento das normas e regulamentos.

O processo de aferição é realizado através de exames de aderência nos processos existentes e documentados, e pode utilizar como base os testes, questionários e treinamentos empregados por afiliadas da Gestora.

D. Acompanhamento dos Processos de Controles Internos:

O Diretor de Compliance, Risco e PLD é responsável por acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos da Gestora.

Adicionalmente, o Diretor de Compliance, Risco e PLD monitorará a qualidade e integridade dos mecanismos de controles internos da Gestora, observado o disposto acima, apresentando eventuais recomendações de aprimoramento de políticas, manuais, práticas e procedimentos que entender necessárias.

O Diretor de Compliance, Risco e PLD também tem acesso regular à capacitação e treinamento dos Colaboradores ou futuros Colaboradores, podendo alterar os critérios, medidas e políticas sem aviso prévio, conforme seu discernimento.

Anualmente, e de acordo com o artigo 25 da Resolução CVM n.º 21, de 25 de fevereiro de 2021 (“Resolução CVM n.º 21/2021”), a Gestora emitirá um relatório de controles internos com a conclusão dos exames efetuados que ficará disponível para a Comissão de Valores Mobiliários (“CVM”) na sede da Gestora.

A Gestora também dispõe de um Comitê de Risco e *Compliance* com atribuição para também deliberar matérias e diretrizes de *Compliance* da gestora e de seus Colaboradores. Contudo, vale ressaltar que a independência do Diretor de Compliance, Risco e PLD é resguardada, podendo discordar de eventuais decisões desse Comitê de Risco e *Compliance* no que tange à assuntos sob sua responsabilidade.

MATERIAL PUBLICITÁRIO

Conforme o art. 21, §2º, da Resolução CVM n.º 175, de 23 de dezembro de 2022 (“Resolução CVM n.º 175/2022”), a Gestora deverá fornecer aos eventuais distribuidores, quando aplicável, todo o material de divulgação dos fundos de investimento e/ou classes dos fundos de investimento.

Nesse sentido, a Gestora deverá observar as regras dispostas na Resolução CVM n.º 175/2022, bem como no Código AGRT. Para tanto, antes de qualquer disponibilização de material

técnico ou publicitário aos distribuidores e prestadores de serviço, referido material deverá ser analisado, verificado e/ou cancelado pela Área de Risco e *Compliance*.

CONFLITOS DE INTERESSE

De forma a evitar possíveis conflitos de interesse, uma vez constatada a incidência ou possibilidade de qualquer conflito, o Diretor de Compliance, Risco e PLD terá comunicação direta com os administradores e sócios da Gestora para realizar relato dos resultados decorrentes das atividades relacionadas a suas funções, incluindo possíveis irregularidades ou falhas identificadas.

Uma vez que os sócios da Gestora podem dispor de participação societária em outras instituições, sempre que for identificado qualquer potencial conflito de interesses, o Diretor de Compliance, Risco e PLD convocará o Comitê de Risco e *Compliance* onde os impactos e os mitigadores serão identificados e definidos.

Adicionalmente, a Gestora entende que eventuais acordos e transações com instituições que seus sócios tenham participação societária, encontram-se em potencial conflito de interesses, devendo ser evitadas e, se realizadas, em bases comutativas.

Caso algum acordo ou transação conflitada seja considerada a melhor oportunidade para seus cotistas, visando a transparência e ética, os cotistas dos veículos geridos serão sempre informados sobre tal acordo ou transação, devendo sua aprovação observar as disposições aplicáveis do Regulamento do fundo participante em tal operação.

CONFLITOS DE INTERESSE – ACORDO DE REMUNERAÇÃO

Na hipótese de existir acordo de remuneração com base na taxa de administração, performance ou gestão, que deve ser paga diretamente pela classe investida a classes investidoras dos fundos de investimento/classes da Gestora, nos termos do inciso XVII do art. 117 da Resolução CVM n.º 175/2022, o valor das correspondentes às parcelas das taxas de administração ou gestão deve ser subtraído e limitado aos valores destinados pela classe investida ao provisionamento ou pagamento das despesas com as referidas taxas.

A Gestora controlará para que o acordo de remuneração não resulte em desconto, abatimento ou redução de taxa de administração, performance, gestão ou qualquer outra taxa devida pela classe investidora à investida dos fundos de investimento sob gestão.

SEGREGAÇÃO DAS ATIVIDADES

A Gestora e suas afiliadas possuem uma equipe própria e independente que atua somente na atividade de *Compliance*.

O Diretor de Compliance, Risco e PLD possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos administradores ou sócios da Gestora ou suas afiliadas.

A Área de *Compliance* atua de forma autônoma e independente, se reportando apenas ao Diretor de Compliance, Risco e PLD indicado na CVM, conforme o disposto no inciso IV, art. 4º, da Resolução CVM nº 21/2021.

Ainda, nos termos da Política de Segregação de Atividades, é vedado que a Gestora tenha acesso ou utilize-se de qualquer informação proveniente de instituições ligadas, seja ela obtida de maneira confidencial/privilegiada ou não, devendo ser assegurada a segregação física, funcional e tecnológica entre as instituições.

INFORMAÇÕES CONFIDENCIAIS

As disposições do presente capítulo se aplicam aos Colaboradores que, por meio de suas funções na Gestora, podem ter ou vir a ter acesso a Informações Confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras, incluindo informações de clientes da Gestora.

Todos os Colaboradores deverão ler atentamente e entender o disposto nesta Política, bem como deverão firmar o termo de confidencialidade, conforme modelo constante do Anexo I (“Termo de Confidencialidade”).

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definida, deve, em qualquer hipótese, ser divulgada fora do âmbito das atividades da Gestora e/ou em desconformidade com o Termo. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da Gestora.

Caso a Gestora venha a contratar terceiros para prestação de serviços e estes venham a ter acesso a Informações Confidenciais, conforme abaixo definido, o contrato de prestação de serviços deverá prever cláusula de confidencialidade.

São consideradas informações confidenciais, reservadas ou privilegiadas (“Informações Confidenciais”), para os fins desta Política, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos de investimentos geridos pela Gestora, incluindo:

- (i) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- (ii) Informações técnicas, financeiras, judiciais ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos fundos de investimentos geridos pela Gestora;
- (iii) Operações estruturadas e demais operações analisadas ou realizadas pelos fundos de investimentos geridos pela Gestora, incluindo, sem limitação, os detalhes da transação, as taxas aplicáveis, garantias, *fees*, partes e valores envolvidos;
- (iv) Informações sobre precatórios e/ou direitos creditórios oriundos de ações judiciais negociados pelos fundos de investimento geridos pela Gestora, incluindo, sem limitação, informações sobre o cedente, o objeto, as partes e terceiros

interessados da lide processual que originou o ativo judicial, deságio e formas de pagamento;

(v) Relatórios, estudos, opiniões internas sobre ativos financeiros;

(vi) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

(vii) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes, 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;

(viii) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimentos geridos pela Gestora;

(ix) Transações realizadas e que não tenham sido divulgadas publicamente; e

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

Sem prejuízo da colaboração da Gestora com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente discutida pela Equipe de Compliance e Risco, para que se decida sobre a forma mais adequada para tal revelação, após exaurir todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Insider Trading, Dicas e Front Running

“*Insider Trading*” significa a compra e venda de títulos ou valores mobiliários com base em informação material e não pública sobre determinado valor mobiliário, incluindo Informação Confidencial, com o objetivo de conseguir benefício próprio ou para terceiros (incluindo os Colaboradores).

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de informação material e não pública sobre determinado valor mobiliário, incluindo Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

“*Front-running*” significa a prática que envolve aproveitar alguma informação privilegiada para realizar ou concluir uma operação antes de outros.

Considerando a natureza dos ativos negociados pelos fundos de investimento geridos pela Gestora, esta entende ser baixo o risco de práticas como *Insider Trading*, *Front Running* ou Dica pelos Colaboradores.

De toda forma, a Gestora negocia ativos judiciais e precatórios, bem como estrutura operações de crédito e, nesse processo, os Colaboradores poderão ter contato com informações materiais e não públicas, incluindo Informações Confidenciais, de companhias que possuam valores mobiliários, representativos de dívida ou *equity*, negociados no mercado. Para mitigar eventuais riscos à Gestora e aos Colaboradores, a Gestora restringe a negociação de tais valores mobiliários por seus Colaboradores, conforme detalhado na Política de Investimentos Pessoais.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança que venham ter necessidade de acessar tal informação também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso, por qualquer meio, a informação material e não pública sobre determinado valor mobiliário, incluindo Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, Risco e PLD, indicando, além disso, a fonte da informação privilegiada assim obtida. Tal dever de comunicação também será aplicável nos casos em que a informação privilegiada seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas com dever de confidencialidade. Os Colaboradores que, desta forma, acessem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance, Risco e PLD.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas nesta Política e na

legislação aplicável, incluindo eventual demissão por justa causa e/ou exclusão do quadro societário da Gestora, conforme aplicável.

PROGRAMA DE SEGURANÇA DA PONTAL CAPITAL

(i) Identificação de Riscos (*risk assessment*):

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – *softwares* desenvolvidos para corromper computadores e redes:
 - *Vírus*: *software* que causa danos a máquina, rede, *softwares* e banco de dados;
 - Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
 - *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e
 - *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
 - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

- *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- Ataques de *DDoS* (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Além de ataques cibernéticos, a Gestora pode estar sujeita ao mau funcionamento dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

Para a identificação e avaliação de riscos, são realizadas as seguintes ações:

- a) Identificação dos ativos relevantes da Gestora (sejam equipamentos, sistemas processos ou dados) usados para seu correto funcionamento;
- b) Avaliação das vulnerabilidades dos ativos, identificando-se possíveis ameaças e graus de exposição;
- c) Mensuração de impacto potencial e probabilidade de ocorrência dos riscos identificados, considerando aspectos financeiros, operacionais e reputacionais.

(ii) Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para a Gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Gestora, em caso de incidente de segurança.

Deste modo, a Gestora segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:

- Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag*:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag*:

- Todas as Informações Confidenciais, a saber:
- *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Gestora;

- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e/ou de seus sócios e clientes.

A partir da definição acima, a Gestora se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag*, *Yellow Flag* e *Green Flag*.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Gestora:

Estrutura de TI

I. Uso dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade e/ou com licenças da Gestora.

II. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da Gestora têm por objetivo o desempenho das atividades profissionais na Gestora.

Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de *softwares* e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área responsável, com supervisão do Diretor de Compliance, Risco e PLD.

A disponibilização e uso dos computadores da Gestora respeitam as seguintes regras:

- A cada novo Colaborador, a área de tecnologia, em consulta com o Diretor de Compliance, Risco e PLD, autorizará, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, *softwares* e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão do Diretor de Compliance, Risco e PLD;
- O Diretor de Compliance, Risco e PLD autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela Gestora é sua assinatura eletrônica no servidor da Gestora;
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A eventual reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes;
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Gestora, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação para a área de tecnologia e/ou ao Diretor de Compliance, Risco e PLD que acionará a primeira.
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma.
- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Compliance, Risco e PLD à área responsável.

III. Softwares

A implantação e configuração de *softwares* da Gestora s respeitam as seguintes regras:

- Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão do Diretor de Compliance, Risco e PLD;
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de tecnologia, em consulta com o Diretor de Compliance, Risco e PLD;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Gestora;
- A conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa da área de tecnologia, em consulta com o Diretor de Compliance, Risco e PLD.

IV. Registros

A Gestora mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela Gestora, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM n.º 21/2021.

V. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Gestora.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da Gestora em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Gestora.

VI. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
- “Log-off” automático por inatividade durante o período de 24 horas;
- Bloqueio do acesso as portas *USB* dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;
- Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud*);
- Bloqueio de sistemas de gerenciamento de computador à distância.

VII. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da Gestora, este deve sempre resguardar a imagem da Gestora, evitando entrar em sites de fontes não seguras, assim como

de abrir e-mails pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de Compliance, Risco e PLD.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Conttenham informações que não colaborem para o alcance dos objetivos da Gestora;
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

O uso de serviços de mensagem instantânea para fins profissionais deve seguir as políticas estabelecidas pelo grupo controlador do Gestora.

Também se faz expressamente proibido o uso de serviços de rádio, *streaming*, *download* de vídeos, filmes e músicas, através dos computadores da Gestora.

VIII. Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Gestora.

IX. Uso de correio eletrônico particular

É proibida a utilização profissional de correio eletrônico particular.

A Gestora disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@pontalcapital.com)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Gestora.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Gestora.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Compliance, Risco e PLD.

X. Endereço eletrônico de programas ou de comunicação corporativa

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Gestora, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da Gestora.

XI. Acesso à distância ao correio eletrônico cedido pela Gestora (e-mail)

O Colaborador pode acessar o seu correio eletrônico cedido pela Gestora mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Gestora.

XII. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na Gestora.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Gestora, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Gestora; e
- Sejam incoerentes com o Código de Ética da Gestora.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Gestora é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Gestora.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

XIII. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Compliance, Risco e PLD.

XIV. Armazenamento em Nuvem (*Cloud*)

A Gestora poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud*).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

XV. Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros (“Terceiros”) podem representar uma fonte significativa de riscos para a Gestora em relação à Cibersegurança. Neste sentido, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem, conforme o nível de diligência previsto nas políticas aplicáveis dos controladores do Gestora.

TESTES PERIÓDICOS DE SEGURANÇA

A Gestora realizará testes periódicos de segurança nos sistemas que armazenam Informações Confidenciais, especialmente aquelas mantidas em meio eletrônico, com periodicidade mínima semestral, incluindo:

- Testes de vulnerabilidade e penetração nos sistemas
- Avaliação de controles de acesso e permissões
- Verificação de logs e auditoria de acessos

A Gestora manterá registro atualizado dos detentores de Informações Confidenciais, identificando nominalmente sócios, administradores, colaboradores e funcionários que possuem acesso a cada categoria de informação (Red Flag, Yellow Flag e Green Flag), para fins de responsabilização em caso de vazamento.

Os resultados dos testes periódicos serão documentados e revisados pelo Diretor de Compliance, Risco e PLD, que implementará as correções necessárias identificadas.

DISPOSIÇÕES GERAIS

Em cumprimento ao art. 16, III, da Resolução CVM n.º 21/2021, a presente Política está disponível no endereço eletrônico disponibilizado pela Gestora para tal fim.

Eventuais comunicações para a Área de *Compliance* devem ser enviadas para o Diretor de Compliance, Risco e PLD.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada periodicamente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Setembro/2025	Carlos Jose Lancellotti Narciso	Versão inicial

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS, E SEGURANÇA CIBERNÉTICA DA PONTAL CAPITAL GESTORA DE RECURSOS LTDA.

Por meio deste instrumento, _____, inscrito no CPF/MF sob o nº _____, (“Colaborador”), e PONTAL CAPITAL GESTORA DE RECURSOS LTDA., inscrita no CNPJ/MF sob o nº 61.893.969/0001-23 (“Gestora” e, em conjunto com o Colaborador, “Partes”), RESOLVEM, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade (“Termo”), que deve ser regido de acordo com as cláusulas que seguem:

1. O Colaborador, desde já, declara que leu e está plenamente de acordo com as disposições da Política de Segurança da Informação, Proteção de Dados, Segurança Cibernética e Confidencialidade da Gestora (“Política”), a qual é parte integral das Regras, Procedimentos e Descrição dos Controles Internos da Pontal Capital.

2. Além do disposto na Política, são consideradas informações confidenciais, reservadas ou privilegiadas (“Informações Confidenciais”), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, *pendrives*, 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, clientes, aqui também contemplados os próprios fundos de investimentos geridos pela Gestora, incluindo:

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

(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos fundos de investimentos geridos pela Gestora;

(iii) Operações estruturadas, e demais operações analisadas, em processo de análise, ou realizadas pelos fundos de investimento geridos pela Gestora, incluindo, sem limitação, os detalhes da transação, as taxas aplicáveis, garantias, *fees*, partes e valores envolvidos;

- (iv) Informações sobre precatórios e outros ativos judiciais já negociados ou em fase de negociação pelos fundos de investimento geridos pela Gestora, incluindo, sem limitação, informações sobre o cedente, o objeto, preço de aquisição e eventuais pagamentos adicionais, as partes e terceiros interessados da lide processual que originou o ativo judicial, deságio e formas de pagamento;
- (v) Relatórios, estudos e opiniões internas sobre ativos financeiros;
- (vi) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- (vii) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes, 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;
- (viii) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimentos geridos pela Gestora;
- (ix) Transações realizadas ou em processo de análise que ainda não tenham sido divulgadas publicamente; e
- (x) Outras informações obtidas junto a sócios, diretores, funcionários ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

3. 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, incluindo para benefício próprio exclusivo e/ou unilateral presente ou futuro para Colaboradores não autorizados, veículos de 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 (“Dever de Confidencialidade”).

3.1. O Colaborador se obriga a, durante a vigência deste Termo e pelo prazo de 5 (cinco) anos após sua rescisão expressa (“Prazo de Confidencialidade”), respeitar o Dever de Confidencialidade, seja atuando em benefício próprio, da Gestora ou de quaisquer terceiros.

4. O Colaborador entende que qualquer violação ao Dever de Confidencialidade durante o Período de Confidencialidade pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Gestora e terceiros, ficando desde já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

4.1. O descumprimento do Dever de Confidencialidade durante o Prazo de Confidencialidade será considerado ilícito civil e criminal, ensejando inclusive na rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis do Trabalho, ou desligamento e exclusão por justa causa, e/ou exclusão do quadro societário da Gestora, conforme aplicável, conforme o vínculo do respectivo Colaborador com a Gestora, obrigando-o, inclusive, a indenizar a Gestora por eventuais prejuízos por esta suportados em decorrência do descumprimento, independentemente das medidas judiciais cabíveis para tanto.

4.2. Independentemente da responsabilização nas esferas cível e criminal, conforme previsto acima, o descumprimento do Dever de Confidencialidade durante o Prazo de Confidencialidade sujeitará o Colaborador à multa não compensatória de até 5% (cinco por cento) sobre o total de remuneração paga pela Gestora (direta ou indiretamente) ao Colaborador nos últimos 3 (três) anos ou sobre o total de remuneração paga pela Gestora (direta ou indiretamente) ao Colaborador, caso não aplicáveis 3 (três) anos, conforme determinação da Equipe de Compliance e Risco.

5. 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, 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 do quadro societário da Gestora e/ou exclusão do quadro societário da Gestora, conforme aplicável, 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.

6. 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.

6.1. 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 a que o Colaborador esteja obrigado a divulgar.

6.2. 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.

7. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

8. Fica eleito o foro da comarca da capital do estado de São Paulo, para dirimir quaisquer disputas decorrentes do presente Termo. Assim, estando de acordo com as condições acima mencionadas, assina o presente na presença das testemunhas abaixo assinadas.

São Paulo, [•] de [•] de [•].

[COLABORADOR]

PONTAL CAPITAL GESTORA DE RECURSOS LTDA.

Carlos Jose Lancellotti Narciso

Testemunhas:

Nome:

Nome:

CPF:

CPF: